DocAve® 6 Supplementary Tools

User Guide

Service Pack 5 Cumulative Update 1

Issued May 2015

Table of Contents

What's New in this Guide 6

Before You Begin 7

Configuration 7

Submitting Documentation Feedback to AvePoint 8

AgentToolSP2010ConnectorCreateList & AgentToolSP2013ConnectorCreateList 9

Generating an Encrypted Password 10

Configuring AgentToolCreateList.csv 10

Configuring AgentToolCreateMySiteAndLibrary.csv 14

Configuring AgentToolCreateWeb.csv 18

Configuring AgentToolCreateSite.csv 21

Configuring AgentToolCreateListForBox.csv 25

Configuring AgentToolCreateListInMysiteForBox.csv 28

Configuring AgentToolCreateListForNFS.csv 33

Working with Configuration Files 36

AgentToolConnectorList.config 37

AgentToolConnectorWeb.config 38

Configuring Inheritance 39

Template Parameter Values 40

Running the AgentToolSP2010ConnectorCreateList or the AgentToolSP2013ConnectorCreateList 41

Manager Tool Dell DX Client 43

Environment Requirements 43

Using the Manager Tool Dell DX Client 43

Manager Tool HCP Client 45

Environment Requirements 45

Using the Manager Tool HCP Client 45

Storage Token Client 47

Using the Storage Token Client 47

Media Service Rebuild Index Tool 48

AgentToolHAMirroringCleanUp 51

Running the AgentToolHAMirroringCleanUp Tool 51
SP2010StorageUpgradeStub 52
Running the SP2010StorageUpgradeStub Tool 52
AgentToolSP2010(2013)MoveStub 53
Running the AgentToolSP2010(2013)MoveStub Tool 53
AgentToolSP2010eDiscoveryMapping & AgentToolSP2013eDiscoveryMapping 57
Permissions Requirements 57
Running the AgentToolSP2010eDiscoveryMapping Tool or the AgentToolSP2013eDiscoveryMapping Tool 57
AgentToolSP2010Connector Tool & AgentToolSP2013Connector Tool 59
Running the AgentToolSP2010Connector Tool or the AgentToolSP2013Connector Tool 59
Operation -o UpgradeVersion 60
Operation -o EncryptPassword 62
Operation -o ReportItems 62
Operation -o UpgradeConnectedLibrary (SharePoint 2013 Only) 63
AgentToolSP2010OrphanStubClean & AgentToolSP2013OrphanStubClean 65
Searching for the Orphan Stubs 65
Cleaning up the Orphan Stubs 67
Replicator Analyzer Tool 68
Deleting Failed Job's Profile Settings Configuration 68
Modifying the Configuration Files in Bulk 69
AgentToolDataTransferGUI 72
System Requirements 72
Enabling Differential Compression 74
Configuring Data Transfer Service Tool 75
Triggering Import Automatically 77
DocAve URL Convert Tool 79
Required Permissions 79
How to Use This Tool 79
Creating the XML File 81
DocAve Migrator Tool 83
Accessing DocAve Migrator Tool 83

File System Migration 83
Configuring Connection Management 83
Configuring File Property Explorer 84
Performing a Scan Analysis 84
Configuring Security Mappings 86
Exchange Public Folder Migration 89
Configuring Exchange Public Folder Connection 90
Scanning 91
Configuring Security Mapping 94
Lotus Notes Migration 96
Configuring Database Connections 96
Exporting DXL File 97
Configuring Content Type Mappings 97
Configuring User Mappings 100
Configuring InfoPath Mappings 105
Performing a Scan Analysis 106
Performing a Database Analysis 109
Viewing Analysis Report 110
Quickr Migration 111
Selecting Source 111
Performing a Scan Analysis 111
Configuring User Mappings 114
Creating a Content Type Mapping 115
Editing an Existing Mapping 115
eRoom Migration 115
Loading eRoom Structure 116
Configuring Security Mapping 116
Performing a Scan Analysis 119
Livelink Migration 122
Performing a Scan Analysis 122
Configuring Security Mappings 131
Configuring Database Inquiry 135

EMC Documentum Migration 136
Configuring EMC Documentum Connection 137
Specifying Source 137
Performing a Scan Analysis 138
Configuring Security Mapping 141
Configuring Content Type Mapping 143
Notices and Copyright Information 145

What's New in this Guide

- Minor edits and cover page update for current release.

Before You Begin

Refer to the sections for system and farm requirements that must be in place prior to using any of the DocAve supplementary tools.

Configuration

In order to use DocAve tools, the DocAve 6 platform and applicable modules must be installed and configured properly on your farm. Some of the tools described in this guide will not function without the DocAve 6 platform and the applicable modules present on the farm.

For instructions on installing the DocAve Platform, DocAve Manager, and DocAve Agents, see the DocAve 6 Installation Guide.

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. You can access the Submit Your Feedback form on our website.

AgentToolSP2010ConnectorCreateList & AgentToolSP2013ConnectorCreateList

The AgentToolSP2010ConnectorCreateList tool (used for SharePoint 2010 environment) and the AgentToolSP2013ConnectorCreateList tool (used for SharePoint 2013 environment) are used to create Connector and Cloud Connect lists in bulk. These tools can also be used to create the sites or site collections that are required to create the lists.

***Note**: If the name of a specific storage folder contains illegal characters, the corresponding list, site, or site collection cannot be created in SharePoint.

The configuration files for this tool support English, German, French, and Japanese language environments. The corresponding configuration files are stored in three folders under *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool* or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool* in *EN*, *GE*, *FR*, and *JP* folders, respectively. Configure the desired configuration files depending on the language of the environment where your Agent is installed.

To use the AgentToolSP2010 or 2013 ConnectorCreateList tool follow the steps below:

1. Generating an Encrypted Password.
2. Configure the .csv file according to your requirements. Only one .csv file is needed to run a command; however, multiple .csv files can be configured to create the site collection, site, etc.
    - Configuring AgentToolCreateList.csv file to set up a Connector library.
    - Configuring AgentToolCreateMySiteAndLibrary.csv file to set up a My Site and libraries within it.
    - Configuring AgentToolCreateWeb.csv file to set up a site with the specified Net Share path.
    - Configuring AgentToolCreateSite.csv file to set up a site collection with the specified Net Share path.
    - Configuring AgentToolCreateListForBox.csv file to set up a Cloud Connect library.
    - Configuring AgentToolCreateListInMysiteForBox.csv to set up a Cloud Connect library in My Site.
    - Configuring AgentToolCreateListForNFS.csv file to set up a Connector library with the specified Network File System storage path.
3. Working with Configuration Files.
4. Running the AgentToolSP2010ConnectorCreateList tool.

Before using this tool, make sure that the BLOB Provider and EBS/RBS settings are properly configured, and that the Connector solutions are successfully deployed (only RBS can be enabled in SharePoint 2013).

Generating an Encrypted Password

Prior to creating any Connector or Cloud Connect libraries using the tool, the password used to connect to the file system must be encrypted using the **AgentToolSP2013Connector** tool, **AgentToolSP2010Connector** tool, or Windows PowerShell. The encrypted password is entered into the .csv files in order to create the Connector or Cloud Connect libraries.

To generate an encrypted password using Windows PowerShell, run `Encrypt-Password`. After you enter the password, the corresponding encrypted password will generate (as shown in the screenshot below).

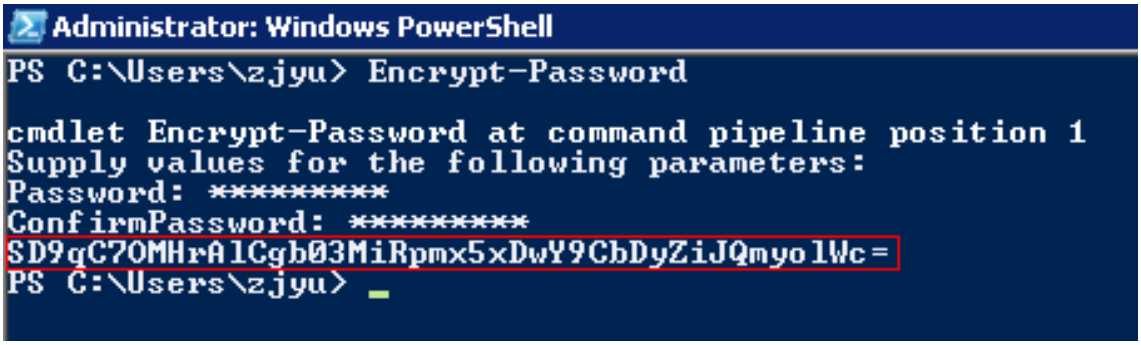


Figure 1: Generating an encrypted password using Windows PowerShell.

To generate an encrypted password using the **AgentToolSP2013Connector** or **AgentToolSP2010Connector** tool, refer to the AgentToolSP2010Connector Tool & AgentToolSP2013Connector Tool section of this user guide for details.

Configuring AgentToolCreateList.csv

Before creating Connector libraries using the **AgentToolSP2010ConnectorCreateList.exe** tool or the **AgentToolSP2013ConnectorCreateList.exe** tool, it is necessary to first configure **AgentToolCreateList.csv**. This file is used to configure Connector libraries (Content Libraries and Media Libraries), and libraries that have been converted to Connector Libraries (Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries).

***Note:** Asset Libraries cannot be converted to Connector Libraries in SharePoint 2013.

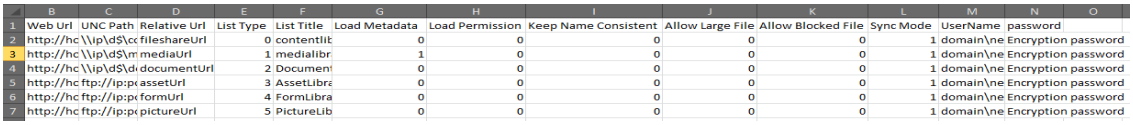
To configure **AgentToolCreateList.csv**, complete the following steps:

1. By default, **AgentToolCreateList.csv** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool for SharePoint*

2010 or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool for SharePoint 2013*. Navigate to this path and select the corresponding language folder.

2. Double-click **AgentToolCreateList.csv** to open the file.

3. The file displays three example rows; these are examples used for creating Content Libraries, Media Libraries, Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries. Remove these rows after entering your own information.



	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Web Url	UNC Path	Relative Url	List Type	List Title	Load Metadata	Load Permission	Keep Name Consistent	Allow Large File	Allow Blocked File	Sync Mode	UserName	password	
2	http://hc	\\ip\d$\cc	fileshareUrl	0	contentlib	0	0	0	0	0	1	domain\ne	Encryption	password
3	http://hc	\\ip\d$\m	mediaUrl	1	medialibr	1	0	0	0	0	1	domain\ne	Encryption	password
4	http://hc	\\ip\d$\d	documentUrl	2	Document	0	0	0	0	0	1	domain\ne	Encryption	password
5	http://hc	ftp://ip:p	assetUrl	3	AssetLibra	0	0	0	0	0	1	domain\ne	Encryption	password
6	http://hc	ftp://ip:p	formUrl	4	FormLibra	0	0	0	0	0	1	domain\ne	Encryption	password
7	http://hc	ftp://ip:p	pictureUrl	5	PictureLib	0	0	0	0	0	1	domain\ne	Encryption	password

Figure 2: Example rows in AgentToolCreateList.csv file for English Environment.

4. Refer to the following table for information that needs to be configured in this file.

Option	Description	Value
Storage Type	The storage type of the Connector library created using the **AgentToolCreateList** tool. ***Note**: If you set the storage type to FTP in this configuration file, the storage settings are automatically synchronized to the newly created Connector library in SharePoint.	Net Share or FTP
Web Url	The URL of the site where you want to create the library. ***Note:** The site specified here must be an existing one. If the site does not exist, create it using SharePoint or using this tool. See Configuring AgentToolCreateWeb.csv for more information.	http://ServerIP:Port/Managed Path/XX/XX
UNC Path	The physical storage path that will be connected to the newly created library.	\\IP\c$\FolderName
Relative Url	The relative URL of the library you want to create.	TestLibrary
List Type	The type of library you want to create. • **0** represents Content Library. • **1** represents Media Library. • **2** represents Document Library. • **3** represents Asset Library (only for SharePoint 2010). • **4** represents Form Library. • **5** represents Picture Library.	0/1/2/3/4/5

Option	Description	Value
List Title	The title of the library you want to create.	TestLibrary
Load Metadata	Specify whether to load metadata from file system to Connector libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1
Load Permission	Specify whether to load the files'/folders' permissions from the file system to Connector libraries during the first synchronization. • **0** represents None; does not load permissions. • **1** only loads the root folder's permissions to replace the permissions of the Connector library. All files and sub-folders under the Connector library inherit the new permissions of the parent node. • **2** loads all of the root folders, sub-folders and files' permissions from the file system and the folders' and files' permissions will be the same as their permissions in the file system.	0/1/2
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Connector library when the filenames are modified due to invalid characters or filename length limitation during the synchronization job. • **0** represents False; does not keep name consistent between Connector library and storage path. • **1** represents True; keeps name consistent between Connector library and storage path.	0/1

Option	Description	Value
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types. • **1** represents True; allows users to upload files of the blocked types.	0/1
Allow Large File	Specify whether to allow data that is larger than X MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files that are larger than X MB to Connector library. • **1** represents True; allows users to upload files that are larger than X MB to Connector library.	0/1

Option	Description	Value
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added, modified, or **deleted** through the SharePoint interface. Only the changes made in SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	1/2
UserName	The account used to set up the access to the specified file system path.	DomainName\UserName
password	The encrypted password for the specified username.	r/6FHm/ jq1iAwlbaGRRTcstAs6HL

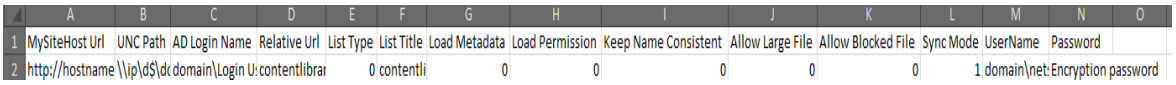
Configuring AgentToolCreateMySiteAndLibrary.csv

AgentToolCreateMySiteAndLibrary.csv is used to configure the library information (Connector libraries, Content Libraries, and Media Libraries), and libraries that have been converted to Connector Libraries (Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries) with the specified Net Share path in the specified My Site.

To configure the AgentToolCreateMySiteAndLibrary.csv, complete the following steps:

1. By default, **AgentToolCreateMySiteAndLibrary.csv** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool for SharePoint 2010* or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool for SharePoint 2013*. Navigate to this path and select the corresponding language folder.

2. Double-click **AgentToolCreateMySiteAndLibrary.csv** to open the file.
3. There is an example row for each option. Remove these rows after entering your own information.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	MySiteHost Url	UNC Path	AD Login Name	Relative Url	List Type	List Title	Load Metadata	Load Permission	Keep Name Consistent	Allow Large File	Allow Blocked File	Sync Mode	UserName	Password	
2	http://hostname	\\ip\d$\dc	domain\Login U	contentlibra	0	contentli	0	0	0	0	0	1	domain\net	Encryption password	

Figure 3: Example rows in AgentToolCreateMySiteAndLibrary.csv file for English Environment.

4. Refer to the following table for information that needs to be configured in this file.

Option	Description	Value
MySiteHost Url	The URL of the My Site host site collection where you want to create the My Sites. ***Note:** The specified site collection here must be an existing one.	http://hostname:port
UNC Path	The exiting physical storage path that will be connected to the newly created library.	\\IP\c$\FolderName
AD Login Name	The username for the AD user who owns the My Site. The format is **domain\user**.	AvePoint\user001
Relative Url	The relative URL of the library you want to create.	TestLibrary
List Type	The type of library you want to create. • **0** represents Content Library. • **1** represents Media Library. • **2** represents Document Library. • **3** represents Asset Library (only for SharePoint 2010). • **4** represents Form Library. • **5** represents Picture Library.	0/1/2/3/4/5
List Title	The title of the library you want to create.	TestLibrary
Load Metadata	Specify whether to load metadata from file system to Connector libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1

Option	Description	Value
Load Permission	Specify whether to load the files'/folders' permissions from the file system to Connector libraries during the first synchronization. • **0** represents None; does not load permissions. • **1** only loads the root folder's permissions to replace the permissions of the Connector library. All files and sub-folders under the Connector library inherit the new permissions of the parent node. • **2** loads all of the root folders, sub-folders and files' permissions from the file system and the folders' and files' permissions will be the same as their permissions in the file system.	0/1/2
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Connector library when the filenames are modified due to invalid characters or filename length limitation during the synchronization job. • **0** represents False; does not keep name consistent between Connector library and storage path. • **1** represents True; keeps name consistent between Connector library and storage path.	0/1
Allow Large File	Specify whether to allow data that is larger than X MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files that are larger than X MB to Connector library. • **1** represents True; allows users to upload files that are larger than X MB to Connector library.	0/1

Option	Description	Value
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types. • **1** represents True; allows users to upload files of the blocked types.	0/1
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added, modified, or **deleted** through the SharePoint interface. Only the changes made in SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	1/2
UserName	The account used to set up the access to the specified file system path.	DomainName\UserName
Password	The encrypted password for the specified username.	r/6FHm/ jq1iAwlbaGRRTcstAs6HL

Configuring AgentToolCreateWeb.csv

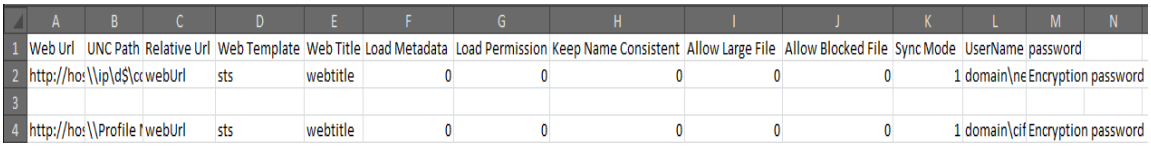
AgentToolCreateWeb.csv is used to configure site information when creating sites with the specified Net Share path.

***Note**: If any Connector libraries are created while a site is being created using this configuration file, the newly created Connector libraries inherit the following Connector settings configured on the site level:

- Load Metadata
- Load Permission
- Keep Name Consistent
- Allow Large File
- Allow Blocked File
- Sync Mode

Refer to the steps below to configure **AgentToolCreateWeb.csv**.

1. By default, **AgentToolCreateWeb.csv** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool for SharePoint 2010 or …\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool for SharePoint 2013*. Navigate to this path and select the corresponding language folder.
2. Double-click **AgentToolCreateWeb.csv** to open the file.
3. By default, there is an example for each option. Remove the example row after entering your own information.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Web Url	UNC Path	Relative Url	Web Template	Web Title	Load Metadata	Load Permission	Keep Name Consistent	Allow Large File	Allow Blocked File	Sync Mode	UserName	password	
2	http://hos	\\ip\d$\cc	webUrl	sts	webtitle	0	0	0	0	0	1	domain\ne	Encryption	password
3														
4	http://hos	\\Profile f	webUrl	sts	webtitle	0	0	0	0	0	1	domain\cif	Encryption	password

Figure 4: Example rows in AgentToolCreateWeb.csv file for English Environment.

4. Refer to the following table for information that needs to be configured in this file.

Option	Description	Value
SiteCollection Url	The URL of the site collection where you want to create the site. ***Note:** The site collection specified here must be an existing one. If it does not exist, first create it using SharePoint or using this tool. Refer to Configuring AgentToolCreateSite.csv for more information.	http://ServerIP:Port/Managed Path/XX

Option	Description	Value
UNC Path	The physical storage path that will be connected to the newly created site.	\\IP\c$\FolderName
Relative Url	The relative URL of the site being created.	TestSite
Web Template	The template of the site you want to create. ***Note**: Site template is the name of the site definition. Site template can be STS, MPS, BLOG, SGS, or the name of a custom type of site. Refer to Template Parameter Values for more information.	sts
Web Title	The title of the site you want to create.	TestSite
Load Metadata	Specify whether to load metadata from file system to Connector libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1
Load Permission	Specify whether to load the files'/folders' permissions from the file system to Connector libraries during the first synchronization. • **0** represents None; does not load permissions. • **1** only loads the root folder's permissions to replace the permissions of the Connector library. All files and sub-folders under the Connector library inherit the new permissions of the parent node. • **2** loads all of the root folders, sub-folders and files' permissions from the file system and the folders and files' permissions will be the same as their permissions in the file system.	0/1/2
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Connector library when the filenames are modified due to invalid characters or filename length limitation during the synchronization job. • **0** represents False; does not keep name consistent between	0/1

Option	Description	Value
	Connector library and storage path. • **1** represents True; keeps name consistent between Connector library and storage path.	
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types. • **1** represents True; allows users to upload files of the blocked types.	0/1
Allow Large File	Specify whether to allow data that is larger than X MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow user to upload files that are larger than X MB to Connector library. • **1** represents True; allows users to upload files that are larger than X MB to Connector library.	0/1
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added, modified, or deleted through **the** SharePoint interface. Only the changes made in SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still	1/2

Option	Description	Value
	regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	
UserName	The account used to set up the access to the specified file system path.	DomainName\UserName
password	The encrypted password for the specified username.	r/6FHm/ jq1iAwlbaGRRTcstAs6HL

Configuring AgentToolCreateSite.csv

AgentToolCreateSite.csv is used to configure site collection information when creating site collections with the specified Net Share path.

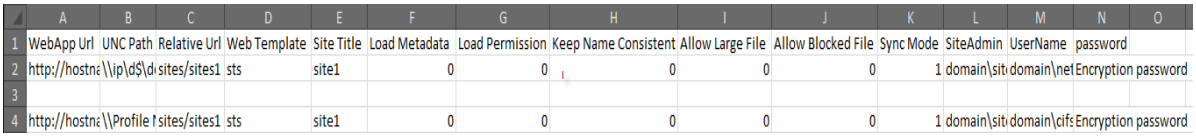
***Note**: If any Connector libraries are created while a site is being created using this configuration file, the newly created Connector libraries inherit the following Connector settings configured on the site level:

- Load Metadata
- Load Permission
- Keep Name Consistent
- Allow Large File
- Allow Blocked File
- Sync Mode

Refer to the steps below to configure **AgentToolCreateSite.csv**.

1. By default, **AgentToolCreateSite.csv** is located in the Agent installation path …*AvePoint**DocAve6**Agent**data**SP2010**Connector**ConnectorCreateListTool for SharePoint 2010 or* …*AvePoint**DocAve6**Agent**data**SP2013**Connector**ConnectorCreateListTool for SharePoint 2013*. Navigate to this path and select the corresponding language folder.
2. Double-click **AgentToolCreateSite.csv** to open the file.

3. By default, there is an example for each option. Remove the example row after entering your own information.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	WebApp Url	UNC Path	Relative Url	Web Template	Site Title	Load Metadata	Load Permission	Keep Name Consistent	Allow Large File	Allow Blocked File	Sync Mode	SiteAdmin	UserName	password	
2	http://hostna	\\ip\d$\d	sites/sites1	sts	site1	0	0	0	0	0	1	domain\sit	domain\net	Encryption	password
3															
4	http://hostna	\\Profile	sites/sites1	sts	site1	0	0	0	0	0	1	domain\sit	domain\cifs	Encryption	password

Figure 5: Example rows in AgentToolCreateSite.csv file for English Environment.

4. Refer to the following table for the information that needs to be configured in this file.

Option	Description	Value
WebApp Url	The URL of the web application where you want to create the site collection. If you want to create a My Site, enter the URL of My Site Host location. ***Note**: The web application specified here must be an existing one. If it does not exist, you must first create it using SharePoint.	http://ServerIP:Port/
UNC Path	The physical storage path that will be connected to the newly created site collection.	\\IP\c$\FolderName
Relative Url	The relative URL of the site collection you want to create. ***Note**: The managed path must be added in front of the relative URL of the site collection.	Managed Path/TestSiteCollection
Web Template	The template of the top-level site of the site collection you want to create. ***Note**: Site template is the name of the site definition. Site template can be STS, MPS, BLOG, SGS, or the name of a custom type of site. Refer to Template Parameter Values for more information.	sts
Site Title	The title of the site collection.	TestSiteCollection
Load Metadata	Specify whether to load metadata from file system to Connector libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1
Load Permission	Specify whether to load the files'/folders' permissions from the file system to Connector libraries during the first synchronization.	0/1/2

Option	Description	Value
	• **0** represents None; does not load permissions. • **1** only loads the root folder's permissions to replace the permissions of the Connector library. All files and sub-folders under the Connector library inherit the new permissions of the parent node. • **2** loads all of the root folders, sub-folders and files' permissions from the file system and the folders and files' permissions will be the same as their permissions in the file system.	
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Connector library when the filenames are modified due to invalid characters or filename length limitation during the synchronization job. • **0** represents False; does not keep name consistent between Connector library and storage path. • **1** represents True; keeps name consistent between Connector library and storage path.	0/1
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types. • **1** represents True; allows users to upload files of the blocked types.	0/1

Option	Description	Value
Allow Large File	Specify whether to allow data that is larger than X MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow user to upload files that are larger than X MB to Connector library. • **1** represents True; allows users to upload files that are larger than X MB to Connector library.	0/1
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added, modified, or deleted through the SharePoint interface. Only the changes made in SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	1/2
SiteAdmin	The account used to create and manage the site collection.	DomainName\UserName
UserName	The account used to set up the access to the specified file system path.	DomainName\UserName
password	The encrypted password for the specified username.	r/6FHm/jq1iAwlbaGRRTcstAs6HL

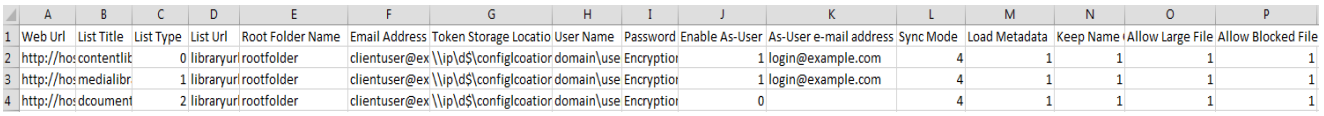
Configuring AgentToolCreateListForBox.csv

Before creating Cloud Connect libraries using the **AgentToolSP2010ConnectorCreateList.exe** tool or the **AgentToolSP2013ConnectorCreateList.exe** tool, it is necessary to first configure **AgentToolCreateListForBox.csv**. This file is used to configure Cloud Connect libraries (Content Libraries and Media Libraries), and libraries that have been converted to Cloud Connect Libraries (Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries).

***Note:** Asset Libraries cannot be converted to Cloud Connect Libraries in SharePoint 2013.

To configure **AgentToolCreateListForBox.csv**, complete the following steps:

1. By default, **AgentToolCreateListForBox.csv** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool for SharePoint 2010 or …\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool for SharePoint 2013*. Navigate to this path and select the corresponding language folder.
2. Double-click **AgentToolCreateListForBox.csv** to open the file.
3. Three example rows are displayed; these are examples used for creating Content Libraries, Media Libraries, Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries. Remove these rows after entering your own information.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Web Url	List Title	List Type	List Url	Root Folder Name	Email Address	Token Storage Locatio	User Name	Password	Enable As-User	As-User e-mail address	Sync Mode	Load Metadata	Keep Name	Allow Large File	Allow Blocked File
2	http://hos	contentlib	0	libraryurl	rootfolder	clientuser@ex	\\ip\d$\configlcoatior	domain\use	Encryptior	1	login@example.com	4	1	1	1	1
3	http://hos	medialibr	1	libraryurl	rootfolder	clientuser@ex	\\ip\d$\configlcoatior	domain\use	Encryptior	1	login@example.com	4	1	1	1	1
4	http://hos	dcoument	2	libraryurl	rootfolder	clientuser@ex	\\ip\d$\configlcoatior	domain\use	Encryptior	0		4	1	1	1	1

Figure 6: Example rows in AgentToolCreateListForBox.csv file for English Environment.

4. Refer to the following table for information that needs to be configured in this file.

Option	Description	Value
Web Url	The URL of the site where you want to create the library. ***Note:** The site specified here must be an existing one. If the site does not exist, create it using SharePoint or using this tool. See Configuring AgentToolCreateWeb.csv for more information.	http://ServerIP:Port/Managed Path/XX/XX
List Title	The title of the library you want to create.	TestLibrary

Option	Description	Value
List Type	The type of library you want to create. • **0** represents Content Library. • **1** represents Media Library. • **2** represents Document Library. • **3** represents Asset Library (only for SharePoint 2010). • **4** represents Form Library. • **5** represents Picture Library.	0/1/2/3/4/5
List Url	The relative URL of the library you want to create.	TestLibrary
Root Folder Name	The folder name you want to synchronize with this library.	RootFolder
Email Address	The e-mail address to access Box.	clientuser@example.com
Token Storage Location	The path of the location where the token's file resides. For details about how to generate the token, refer to Storage Token Client.	\\ip\d$\configlcoation
User Name	The username to access the token storage location.	domain\user
Password	The encrypted password of the specified user.	r/6FHm/jq1iAwlbaGRRTcstAs6HL
Enable As-User	Choose whether to use the current user to access other account's Box storage location. • **0** represents disabled; cannot access other account's Box storage location. • **1** represents enable; enable to access other account's Box storage location.	0/1
As-User e-mail address	The e-mail address of the user whose Box data you want to view and manage.	login@example.com

Option	Description	Value
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added, modified, or **deleted** through the SharePoint interface. Only the changes made in SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	
Load Metadata	Specify whether to load metadata from file system to Cloud Connect libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1

Option	Description	Value
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Cloud Connect library when the filenames are modified due to invalid characters or filename length limitation during the synchronization job. • **0** represents False; does not keep name consistent between Cloud Connect library and storage path. • **1** represents True; keeps name consistent between Cloud Connect library and storage path.	0/1
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types. • **1** represents True; allows users to upload files of the blocked types.	0/1
Allow Large File	Specify whether to allow data that is larger than **X** MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files that are larger than X MB to Cloud Connect library. • **1** represents True; allows users to upload files that are larger than X MB to Cloud Connect library.	0/1

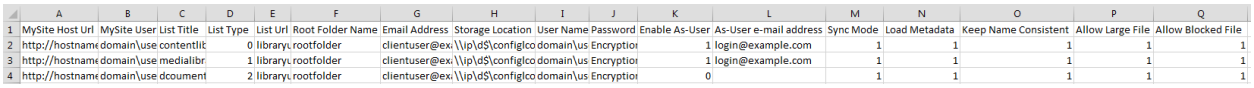
Configuring AgentToolCreateListInMysiteForBox.csv

AgentToolCreateListInMysiteForBox.csv is used to configure the library information (Cloud Connect libraries (Content Libraries and Media Libraries), and libraries that have been converted to Cloud

Libraries (Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries)) with the specified Box storage location in the specified My Site.

To configure the AgentToolCreateListInMysiteForBox.csv, complete the following steps:

1. By default, **AgentToolCreateListInMysiteForBox.csv** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool* or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool.* Navigate to this path and select the corresponding language folder.
2. Double-click **AgentToolCreateListInMysiteForBox.csv** to open the file.
3. There are three example rows for each option. Remove these rows after entering your own information.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	MySite Host Url	MySite User	List Title	List Type	List Url	Root Folder Name	Email Address	Storage Location	User Name	Password	Enable As-User	As-User e-mail address	Sync Mode	Load Metadata	Keep Name Consistent	Allow Large File	Allow Blocked File
2	http://hostname	domain\use	contentlib	0	library	rootfolder	clientuser@ex	\\ip\d$\configlo	domain\us	Encryptio	1	login@example.com	1	1	1	1	1
3	http://hostname	domain\use	medialibr	1	library	rootfolder	clientuser@ex	\\ip\d$\configlo	domain\us	Encryptio	1	login@example.com	1	1	1	1	1
4	http://hostname	domain\use	dcument	2	library	rootfolder	clientuser@ex	\\ip\d$\configlo	domain\us	Encryptio	0		1	1	1	1	1

Figure 7: Example rows in AgentToolCreateListInMysiteForBox.csv file for English Environment.

Option	Description	Value
MySite Host Url	The URL of the My Site host site collection where you want to create the My Sites. ***Note:** The specified site collection here must be an existing one.	http://hostname:port
MySite User	The username for the user who owns the My Site. The format is **domain\user**.	AvePoint\user
List Title	The title of the library you want to create.	TestLibrary
List Type	The type of library you want to create. • **0** represents Content Library. • **1** represents Media Library. • **2** represents Document Library. • **3** represents Asset Library (only for SharePoint 2010). • **4** represents Form Library. • **5** represents Picture Library.	0/1/2/3/4/5
List Url	The relative URL of the library you want to create.	TestLibrary

Option	Description	Value
Root Folder Name	The folder name you want to synchronize with this library.	RootFolder
Email Address	The e-mail address to access Box.	clientuser@example.com
Storage Location	The path of the location where the token's file resides. For details about how to generate the token, refer to Storage Token Client.	\\ip\d$\configlcoation
User Name	The username to access the token storage location.	domain\user
Password	The encrypted password of the specified user.	r/6FHm/jq1iAwlbaGRRTcstAs6HL
Enable As-User	Choose whether to use the current user to access other account's Box storage location. • **0** represents disabled; cannot access other account's Box storage location. • **1** represents enable; enable to access other account's Box storage location.	0/1
As-User e-mail address	The e-mail address of the user whose Box data you want to view and manage.	login@example.com
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added, modified, or **deleted** through the SharePoint interface. Only the changes made in	1/2

Option	Description	Value
	SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	
Load Metadata	Specify whether to load metadata from file system to Cloud Connect libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Cloud Connect library when the filenames are modified due to invalid characters or filename	0/1

Option	Description	Value
	length limitation during the synchronization job. • **0** represents False; does not keep name consistent between Cloud Connect library and storage path. • **1** represents True; keeps name consistent between Cloud Connect library and storage path.	
Allow Large File	Specify whether to allow data that is larger than **X** MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files that are larger than X MB to Cloud Connect library. • **1** represents True; allows users to upload files that are larger than X MB to Cloud Connect library.	0/1
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types.	0/1

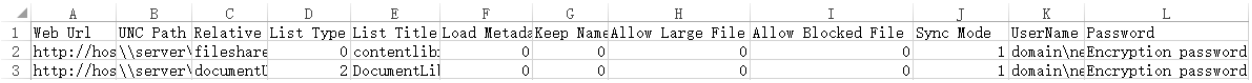
Option	Description	Value
	• **1** represents True; allows users to upload files of the blocked types.	

Configuring AgentToolCreateListForNFS.csv

AgentToolCreateListForNFS.csv is used to configure the library information (Content Libraries, Media Libraries, and libraries that have been converted to Connector Libraries (Document Libraries, Asset Libraries, Form Libraries, and Picture Libraries)) with the specified Network File System storage path in the specified Site collection.

To configure the **AgentToolCreateListForNFS.csv**, complete the following steps:

1. By default, **AgentToolCreateListForNFS.csv** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool* or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool.* Navigate to this path and select the corresponding language folder.
2. Double-click **AgentToolCreateListForNFS.csv** to open the file.
3. There are two example rows for each option. Remove these rows after entering your own information.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Web Url	UNC Path	Relative	List Type	List Title	Load Metad	Keep Name	Allow Large File	Allow Blocked File	Sync Mode	UserName	Password
2	http://hos	\\server\	fileshare	0	contentlib	0	0	0	0	1	domain\ne	Encryption password
3	http://hos	\\server\	documentL	2	DocumentLil	0	0	0	0	1	domain\ne	Encryption password

Figure 8: Example rows in AgentToolCreateListForNFS.csv file for English Environment.

4. Refer to the following table for information that needs to be configured in this file.

Option	Description	Value
Web Url	The URL of the site where you want to create the library. ***Note:** The site specified here must be an existing one. If the site does not exist, create it using SharePoint or using this tool. See Configuring AgentToolCreateWeb.csv for more information.	http://ServerIP:Port/Managed Path/XX/XX
UNC Path	The Network File System storage path that will be connected to the newly created library.	\\server\shared folder

Option	Description	Value
Relative Url	The relative URL of the library you want to create.	TestLibrary
List Type	The type of library you want to create. • **0** represents Content Library. • **1** represents Media Library. • **2** represents Document Library. • **3** represents Asset Library (only for SharePoint 2010). • **4** represents Form Library. • **5** represents Picture Library.	0/1/2/3/4/5
List Title	The title of the library you want to create.	TestLibrary
Load Metadata	Specify whether to load metadata from file system to Connector libraries during the first synchronization. • **0** represents False; does not load the metadata. • **1** represents True; load the metadata.	0/1
Keep Name Consistent	Specify whether to keep the filenames in the storage path consistent with those in the Connector library when the filenames are modified due to invalid characters or filename length limitation during the synchronization job. • **0** represents False; does not keep name consistent between Connector library and storage path. • **1** represents True; keeps name consistent between	0/1

Option	Description	Value
	Connector library and storage path.	
Allow Large File	Specify whether to allow data that is larger than X MB (X means the current Web application maximum upload size) to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files that are larger than X MB to Connector library. • **1** represents True; allows users to upload files that are larger than X MB to Connector library.	0/1
Allow Blocked File	Specify whether to allow files of blocked types to be connected from the storage device and synchronized between the storage device and SharePoint. • **0** represents False; does not allow users to upload files of the blocked types. • **1** represents True; allows users to upload files of the blocked types.	0/1
Sync Mode	Select the Synchronization mode that will be used. There are three synchronization modes to be selected. • **1** represents **sync changes made in SharePoint to the storage path** – It is used if files are only being added,	1/2

Option	Description	Value
	modified, or **deleted** through the SharePoint interface. Only the changes made in SharePoint will be synchronized to the storage path if **1** is configured. • **2** represents **sync changes made in SharePoint to the storage path and load new files from the storage path** – It is used if files are being added, modified, or deleted through the SharePoint interface, and files are still regularly being added to the storage location. If the value is set as **2**, the changes made in SharePoint will be synchronized to the storage path, and the newly added files in the storage path will be synchronized to SharePoint.	
UserName	The account used to set up the access to the specified Network File System path.	domain\netshareuser
Password	The encrypted password of the specified user.	r/6FHm/jq1iAwlbaGRRTcstAs6HL

Working with Configuration Files

When creating site collections or sites using the AgentToolSP2010ConnectorCreateList tool (for SharePoint 2010) or the AgentToolSP2013ConnectorCreateList tool (for SharePoint 2013), the file system path must be provided in the corresponding .csv files. If there are sub-folders under the specified

file system path, by default, the sub-folders are created as Content Libraries in SharePoint; however, the sub-folder can also be converted to other types of libraries or sites by editing the two configuration files, **AgentToolConnectorList.config** and **AgentToolConnectorWeb.config**.

The two configuration files, **AgentToolConnectorList.config** and **AgentToolConnectorWeb.config**, are located in *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool* or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool***.** To edit these files, see the appropriate section below.

AgentToolConnectorList.config

To create a sub-folder to use as a Connector library (Content Library/Media Library), Document Library, Asset Library, Form Library, or Picture Library, modify the **AgentToolConnectorList.config** file as described below.

1. By default, **AgentToolConnectorList.config** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool* or *…\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool*. Navigate to the corresponding path according to your SharePoint versions.
2. Right-click **AgentToolConnectorList.config** and choose to open the file with Notepad.

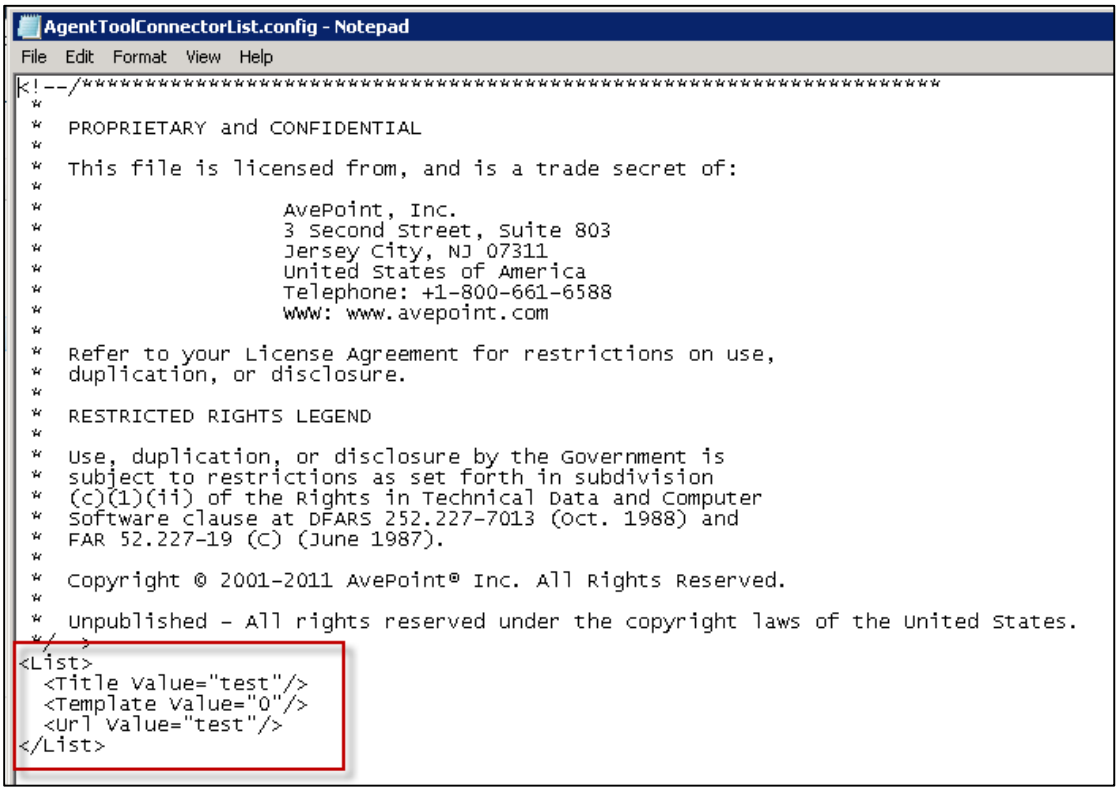


Figure 9: Values to modify in AgentToolConnectorList.config file.

3. In the *<List>* node, modify the *Title Value*, *Template Value*, and *Url Value* according to your requirements.

Property	Description	Value
Title Value	The name of the library you want to create.	test
Template Value	The template of the library you want to create. • **0** represents Content Library. • **1** represents Media Library. • **2** represents Document Library. • **3** represents Asset Library (only for SharePoint 2010). • **4** represents Form Library. • **5** represents Picture Library.	0/1/2/3/4/5
Url Value	The relative URL of the library you want to create.	test

4. When finished, copy the modified **AgentToolConnectorList.config** file to the target sub-folder.

AgentToolConnectorWeb.config

To create a site based on a sub-folder, modify the **AgentToolConnectorWeb.config** file as described below:

1. By default, **AgentToolConnectorWeb.config** is located in the Agent installation path *…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool or …\AvePoint\DocAve6\Agent\data\SP2013\Connector\ConnectorCreateListTool*. Navigate to the corresponding path according to your SharePoint versions.
2. Right-click **AgentToolConnectorWeb.config** and choose to open the file with Notepad.

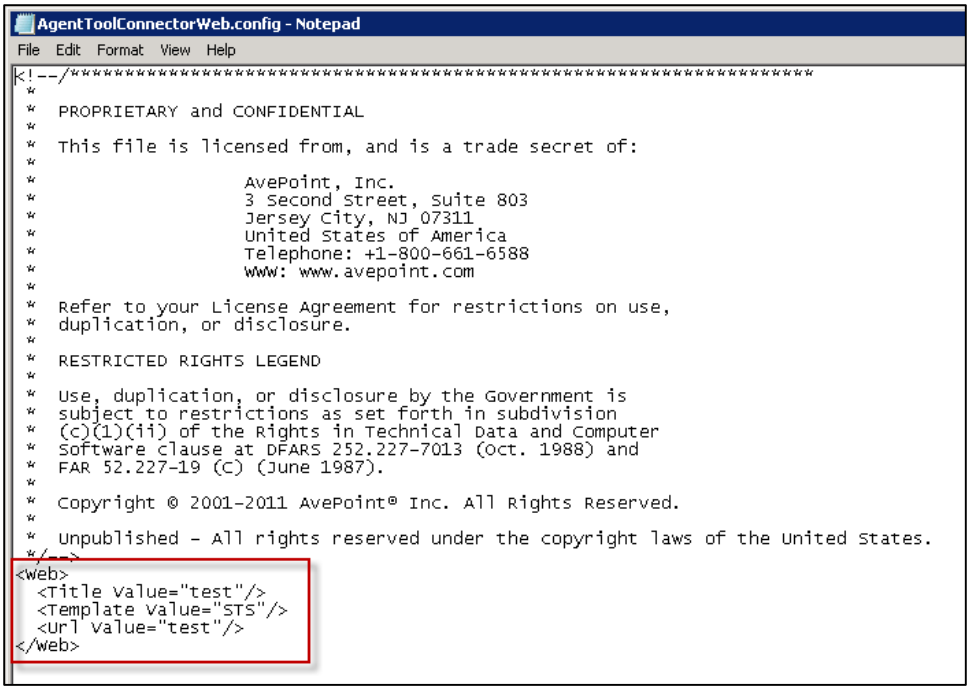


Figure 10: Values to modify in AgentToolConnectorWeb.config file.

3. In the **<Web>** node, modify the **Title Value**, **Template Value**, and **Url Value** according to your requirements.

Property	Description	Value
Title Value	The title of the site you want to create.	test
Template Value	The template of the site you want to create. ***Note**: Site template is the name of the site definition. Site template can be STS, MPS, BLOG, SGS, or the name of a custom type of site. Refer to Template Parameter Values for more information.	sts
Url Value	The relative URL of the site you want to create.	test

4. When finished, copy the modified **AgentToolConnectorWeb.config** file to the target sub folder.

Configuring Inheritance

Use the files **AgentToolConnectorList.config** and **AgentToolConnectorWeb.config** to configure the URL of the current folder (the folder that will house the configuration file) to inherit the folder name from file system or break the inheritance.

- If the node **<Url Value=””/>** in the configuration file is set to “null” or the name of the current folder, the URL inherits the name of the current folder from the file system.

- If the node **<Url Value=””/>** in the configuration file is set to other values instead of the name of the current folder, the URL breaks the inheritance and creates a relative URL using the URL value you provide.

Template Parameter Values

Refer to the following table for the parameter value of each top-level site template.

Template Name	Parameter Value
Team Site	STS#0
Blank Site	STS#1
Document Workspace	STS#2
Blog	BLOG#0
Group Work Site	SGS#0
Visio Process Repository	visprus#0
Basic Meeting Workspace	MPS#0
Blank Meeting Workspace	MPS#1
Decision Meeting Workspace	MPS#2
Social Meeting Workspace	MPS#3
Multipage Meeting Workspace	MPS#4
Document Center	BDR#0
Records Center	OFFILE#1
Business Intelligence Center	BICenterSite#0
Enterprise Search Center	SRCHCEN#0
My Site Host	SPSMSITEHOST#0
Basic Search Center	SRCHCENTERLITE#0/SRCHCENTERLITE#1
FAST Search Center	SRCHCENTERFAST#0
Publishing Portal	BLANKINTERNETCONT
Enterprise Wiki	ENTERWIKI#0

Refer to the following table for the parameter value of each site template.

Template Name	Parameter Value
Team Site	STS#0
Blank Site	STS#1
Document Workspace	STS#2
Blog	BLOG#0
Group Work Site	SGS#0
Visio Process Repository	visprus#0
Basic Meeting Workspace	MPS#0
Blank Meeting Workspace	MPS#1
Decision Meeting Workspace	MPS#2
Social Meeting Workspace	MPS#3
Multipage Meeting Workspace	MPS#4
Document Center	BDR#0

Template Name	Parameter Value
Records Center	OFFILE#1
Basic Search Center	SRCHCENTERLITE#1
Assets Web Database	ACCSRV#1
Charitable Contributions Web Database	ACCSRV#3
Contacts Web Database	ACCSRV#4
Issues Web Database	ACCSRV#6
Personalization Site	SPSMSITE#0
Projects Web Database	ACCSRV#5

Running the AgentToolSP2010ConnectorCreateList or the AgentToolSP2013ConnectorCreateList

After completing the necessary configurations, refer to the steps below to create Connector libraries using the **AgentToolSP2010ConnectorCreateList.exe** tool or the **AgentToolSP2013ConnectorCreateList.exe** tool.

***Note**: The account used to run this tool must be the Farm administrator.

1. Navigate to the tool location; by default, this tool is located in the Agent installation path *…\AvePoint\DocAve6\Agent\bin*.
2. In the Command Line Window, enter the command including the path of the tool **AgentToolSP2010ConnectorCreateList.exe** or **AgentToolSP2013ConnectorCreateList.exe**, the path of the .csv file **AgentToolCreateList.csv**, the path where you want to store the report file generated by this tool, and the thread number that specifies how many libraries you want to create concurrently. The thread number cannot be more than 5. For example,

   "X:\…\AvePoint\DocAve6\Agent\bin\AgentToolSP2010ConnectorCreateList.exe" –c "X:\…\AvePoint\DocAve6\Agent\data\SP2010\Connector\ConnectorCreateListTool\AgentToolCreateList.csv" -r "X:\...\report" -t X

   Figure 11: Example of running the AgentToolSP2010ConnectorCreateList.exe.

   ***Note**: The generated report lists Operation, FileSystem Path, Parent Url, Relative Url, Title, Result, and Exception information. In addition, the creating and saving result statistics are also collected.

3. After you run the command, the window displays the real-time job progress. You can check whether it is creating or saving lists and whether the operation is successful.

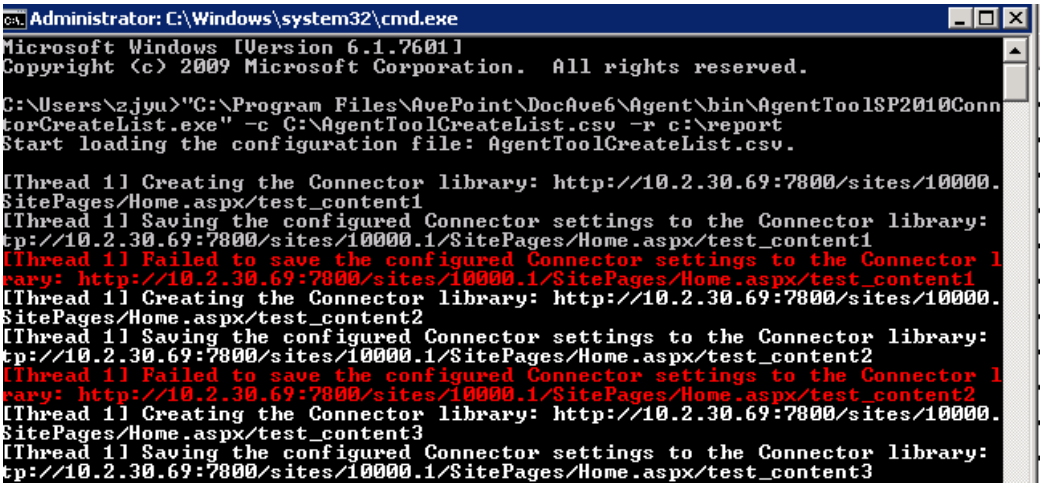


Figure 12: Real-time job progress in the command line window.

The command for creating the site/site collection that is connected to the specified path is similar to the command for creating the Connector library. However, ensure that you change the .csv file to **AgentToolCreateWeb.csv** or **AgentToolCreateSite.csv** accordingly and remove the thread number, as only one site/site collection can be created concurrently.

Manager Tool Dell DX Client

Use the **ManagerToolDELLDXClient** tool to display and update the **retention time**, **compression type**, and the **date of deferred compression** of DocAve Archiver data that is saved on a Dell DX Storage server.

***Note**: Only **Finished** jobs can be loaded in the farm tree and processed by this tool. The data of **Finished with Exception** jobs or **Failed** jobs will not be loaded nor processed.

Environment Requirements

- .Net Framework 3.5 or above.
- The machine on which you run this tool must be within the same subnet as the Dell DX Storage server.

Using the Manager Tool Dell DX Client

To use the tool, complete the following steps:

1. Navigate to *…\AvePoint\DocAve6\Manager\Shared\Tools\DELLDXClient* and locate the **ManagerToolDELLDXClient.exe** file.
2. Right-click **ManagerToolDELLDXClient.exe** and select **Run as administrator** to run the tool.
3. Enter the **hostname** or **IP address** of the DocAve Control Service in the **DocAve Control Service Host** field.
4. Enter the DocAve Control Service port into the **DocAve Control Service Port** field. By default, DocAve uses **14000** as the Control Service port.
5. Enter the username and the password that are used to log into DocAve into the **Username** and **Password** fields, respectively.
6. Select a DocAve module from the **Component** drop-down box. By default, **Archiver** is selected.
7. Click **Load** to load the jobs' information of the specified module. The information for all of the completed jobs is shown on the left side of the screen. Click **Reset** to clear or reset all of the information in the two areas to their default values.
8. Double-click one job on the tree; the **Original Retention Date**, **Original Compression Type**, and the **Original Defer Compression** date of the specified job is shown in the corresponding area on the right.
9. Select one or several jobs on the tree. You can modify the retention date, compression type, and the date that the compression is deferred to in the right area of the interface.

   ***Note**: You can select several jobs to run at the same time, but only the jobs that meet the conditions will be processed by this tool. Refer to the report to view the job status.

- **Month to Extend** – Enter a positive integer in the field and click **Update Retention Date** to postpone the original retention date for the specified number of months.

  For example, enter **3** in the **Month to Extend** textbox. If the **Original Retention Date** displayed in the tool is **Sat, 13 Aug 2011 02:28:32 GMT**, after clicking the **Update Retention Date** button, the original retention date will be postponed for 3 months. The new retention date is **Sun, 13 Nov 2011 02:28:32 GMT**.

  ***Note**: If no retention time was set initially, no action will be performed by the tool.

- **New Compression Type** – Select the new compression type from the drop-down box and click **Update Compression Type**. The original compression type is replaced with the new one.
  - **No** means that the data will not be compressed.
  - **Fast** means that the compression time is shorter, but the size of the data will not be reduced too much because the compress rate is low.
  - **Best** means the size of the data will be greatly reduced; however, the compression time is longer.

  ***Note**: If the new compression type you selected is the same as the old one, no action will be performed by the tool.

- **Delay Compression Until** – Enter a positive integer in the field and click **Update Defer Compression**. The original date that the compression is deferred to will be postponed for the specified days.

  For example, enter **3** in the **Delay Compression Until** text box.

  - If the compression setting is not enabled or the file is already compressed, no action will be performed by the tool.
  - If the compression setting is enabled and the file is not compressed, the compression time will be reset to three days later from the current time.

10. The progress of the update job is shown in the progress bar at the bottom of the tool.
11. After all of the update jobs finish, click **Exit** to exit the tool. You can view the logs and detailed reports of the jobs in the **logs.txt** and **reports.txt** files, accordingly. The files reside in the same folder as the **ManagerToolDELLDXClient.exe** file.

Manager Tool HCP Client

This tool is used to display and update the properties (Retention time, Hold, Shred, and Index) of DocAve Archiver data that is saved on an HDS Hitachi Content Platform server.

Environment Requirements

- .Net Framework 3.5 or above.

Using the Manager Tool HCP Client

Refer to the steps below to use the tool.

1. Navigate to *…\AvePoint\DocAve6\Manager\Shared\Tools\HCPClient* on the DocAve Control server to locate the **ManagerToolHCPClient.exe** file.
2. Right-click **ManagerToolHCPClient.exe** and select **Run as administrator** to run the tool.
3. Enter the **hostname** or **IP address** of the DocAve Control server in **DocAve Control Service Host** text box.
4. Enter the DocAve Control service **port** into the **DocAve Control Service Port** text box. By default, DocAve uses **14000** as the Control service port.
5. Enter the username and the password that are used to login DocAve into the **Username** and **Password** text boxes.
6. Select a **module** in the **Component** drop-down box. By default, **Archiver** is selected.
7. Click **Load** to load the jobs' information of the specified module. The information of all the completed jobs will be shown in the left area. Click **Reset** to and all the information displayed in the tool will be cleared or reset to the default value.
8. Double-click one job on the tree; detailed information on the selected job will be shown in the corresponding area on the right.
9. Select one or several jobs on the tree. You can modify the following settings in the right area.
    - **Index** – Select whether to enable the index feature on the HDS Hitachi Content Platform server. If this value is set to **true**, the detailed metadata of archived data can be searched using the index. By default, this feature is enabled.

      Select **true** to enable this feature and select **false** to disable it.

    - **Shred** – Select whether to enable the shred feature of the HDS Hitachi Content Platform server. By default, this feature is not enabled.
        - If you configure this vaue as **true** and run the update, archived data will be deleted thoroughly when the retention time is reached. The deleted data cannot not be restored.

- If you configure this value as **true** and run the update, the value cannot be configured as **false** in later jobs.

Select **true** to enable this feature and select **false** to disable it.

- **Month/Day/Hour to Extend** – Enter a positive integer in the text box and click **Update**. The original retention date will be postponed for the specified time.

  If the original retention date (**Retention** column) displayed in the tool is **Thursday, 19 Jan 2012 02:28:32 GMT** and you enter 3 in the **Month to Extend** text box, after clicking the **Update** button, the original retention date will be postponed for 3 months. The new retention date is **Thursday, 19 Apr 2012 02:28:32 GMT**.

  ***Note**: If no retention time has been set in the past, no action will be performed by the tool.

- **Hold** – Enable the **Hold** feature to protect the data from being deleted. Once the data is held, it cannot be deleted by end-users, and any retention job will affect the held data. You cannot expand the retention date of the held data.

  Select **true** to enable this feature and select **false** to disable it.

10. Click **Update** to run the update job. The status of the update job will be shown at the bottom of the tool.

After all update jobs finish, click the **Report** button to view the summary report of the job or click **Show Details** button to view details of the job in the tool. Click to exit the tool.

Storage Token Client

Use the **StorageTokenClient** tool to generate the token that is used when configuring the Box, Dropbox, Google Drive, or OneDrive type physical device.

***Note:** .Net Framework 3.5 or above is required for the environment.

Using the Storage Token Client

To use the Storage Token Client, complete the following steps:

1. Navigate to …*DocAve6**Manager**Shared**Tools**StorageTool**StorageTokenTool* on the DocAve Control server to locate the **StorageTokenClient.exe** file.
2. Right-click **StorageTokenClient.exe** and select **Run as administrator** to run the tool.
3. In the **API Verification** page, select a physical device type from the **Storage Type** drop-down list.
4. Click the link on this page to get the application information.
5. Enter the **Client ID**, **Client Secret** and **Redirect URL** into the corresponding text box.

   ***Note:** For Box type physical device, only enter the **Client ID** and **Client Secret** into the corresponding text box. For Dropbox type physical device, enter the **App Key**, **App Secret** and **Redirect URL** into the corresponding text box.
6. Click **Next** and the **Login** page appears.
7. Enter the e-mail address and password to sign in.
8. Click **Generate** once you have connected.
9. The token is generated automatically and displayed in the **Token** page.

   ***Note:** For Box type physical device, there is a link displayed in the **Token** page.
10. Click **Copy** to copy the generated token that is used when configuring the Dropbox/Google Drive/OneDrive type physical device in DocAve Control Panel.

    ***Note:** For Box type physical device, click the link displayed on the **Token** page and then select a storage location for the generated configuration file that stores the tokens and this path can be used when configuring the Box type physical device in DocAve Control Panel.
11. Click **Finish** to exit this wizard.

***Note:** To use this tool to generate the token that is used when configuring the Box type physical device, ensure https://e1.boxcdn.net, https://e2.boxcdn.net, https://sso.services.box.net, https://app.box.com, https://www.avepointonlineservices.com, https://www.box.com, and https://api.box.com can be accessed by the server where the **StorageTokenClient** tool resides to help the **StorageTokenClient** tool run successfully.

Media Service Rebuild Index Tool

This tool is used to rebuild crashed index files for the backup and/or archived data. The **MediaServiceRebuildIndexTool.exe** works with the data of DocAve Granular Back and Restore, Platform Backup and Restore, and Archiver.

Refer to the instructions below for more information on using **MediaServiceRebuildIndexTool.exe**:

1. Navigate to *…AvePoint\DocAve6\Manager\Media\bin* on the server where the Media service resides.
2. Right-click **MediaSerivceRebuildIndexTool.exe** and select **Run as administrator** to run the tool. The **Index Rebuild Tool** interface appears.

There are two index configuration modes: **Manual** and **Automatic**:

- **Manual** mode requires the user to manually enter the Net Share directory where the backup or archived data resides and specify the destination path information where you want to store the index files. After executing the tool, the index files will be rebuilt based on the backup or archived data, and be stored to the specified Net Share index location.
- **Automatic** mode helps the users rebuild the index for the backup or archived data stored in Net Share or TSM storage type, based on the storage policy you choose. It will store the rebuilt index file to the specified logical device.

Manual mode supports to rebuild the index file for the data stored in Net Share; **Automatic** mode supports to rebuild the index file for the data stored in Net Share or TSM. Refer to the section below for more information on using the two different modes.

To rebuild the index by using **Manual** mode, complete the following steps:

1. Select the **Manual** radio button, and then click **Next** to go to the Manual mode **Index Rebuild Tool** interface.
2. Select the backup type from the **Backup Type** drop-down list. The **Manual** mode supports the following backup types: **Archiver (Data Level Rebuild)**, **Archiver (Index Level Rebuild)**, **Granular**, and **Platform**.
3. In the **Data Information** area, enter the net share directory of the backup data in the **Data Path** text box in the format: *\\admin-pc\c$\data_granular\FarmName\PlanId\CycleId\JobId*.
4. Specify the **Username** and **Password** into the corresponding text boxes to access the specified data path.
5. Click **Validation Test** to check whether the data path is available.
6. In the **Index Information** area, enter the net share directory where you want to store the index files in the format: *\\admin-pc\c$\data_granular\FarmName\PlanId\CycleId*.
7. Specify the **Username** and **Password** into the corresponding text boxes to access the specified index path.

8. Click **Validation Test** to check whether the index path is available.
9. Click **Start** to rebuild the index. Click **Back** to return to the launch window of the tool.

If you want to run this tool in **Automatic** mode, make sure that the DocAve Control service is available. To rebuild the index files in batches for the backup data by using **Automatic** mode, complete the following steps:

1. Select the **Automatic** radio button, and then enter the login ID and password of the DocAve built-in account into the **Login ID** text box and the **Password** text box.
2. Click **Next** to go to the Automatic mode **Index Rebuild Tool** interface.
3. Select the backup type from the **Backup Type** drop-down list. The Automatic mode supports the following backup types: **Archiver**, **Granular**, and **Platform**.
4. In the **Data Information** area, select the storage policy from the **Storage Policy** drop-down list, where the backup data with corrupted index files resides. Expand the data tree. For Archiver backup type, select the site collection from the archived data tree. For Granular and Platform, select the Job IDs of the backup data from the backup data tree.

   ***Note**: **Automatic** mode supports to rebuild index for the data in the storage policies that are using **Net Share** or **TSM** as the **Storage Type**.

   ***Note:** AvePoint does not recommend only selecting the Incremental Backup or Deferential Backup jobs without the Full Backup jobs to rebuild the index files. Otherwise, errors may occur on the destination after the restore job based on these backup data completes.
5. In the **Index Information** area, select a logical device from the drop-down list to store the index files.

   ***Note**: Granular and Platform backup types support the logical device using **Net Share** or **TSM** storage type. Archiver only supports the logical device using **Net Share** storage type.
6. Click **Start** to rebuild the index files. Click **Back** to return to the launch window.

   ***Note:** Before rebuilding the index files of the backup data, ensure that no backup job or restore job relating to the same cycle of the selected backup data is currently running.

   If any scheduled jobs relating to this cycle will be started in the rebuilding process, AvePoint recommends stopping the DocAve Timer Service during this period or stopping the scheduled job in **Job Monitor**.

After the rebuilding process is finished, the index files of the selected backup data are generated in the physical device of the specified logical device and the newly generated index files has replaced the former index files.
***Note:** The Rebuild Index Tool does not support rebuilding the index file for the backup data without available .dat files.

***Note:** After using this tool to rebuild the index for the selected backup data whose index file was deleted or corrupted, the first Incremental Backup or Deferential Backup job related to the selected backup data will be forced to perform a Full Backup, which may take a while.

***Note:** The Rebuild Index Tool does not support rebuilding the index file for the backup data of the Platform Backup and Restore jobs without available catalog.idx files.

AgentToolHAMirroringCleanUp

This tool helps users clean up the **Restoring** databases, certificate, endpoint, login, user, and master keys for the database mirroring relationships in the specified SQL server.

Running the AgentToolHAMirroringCleanUp Tool

1. Navigate to …*AvePoint**DocAve6**Agent**bin,* and locate the **AgentToolHAMirroringCleanUp.exe**.
2. Right-click the **AgentToolHAMirroringCleanUp.exe**, and then select **Run as administrator** to run this tool.
3. In the **DocAve High Availability Mirroring Clean Up Tool** interface, enter the SQL server instance name into the **Server name** text box.
4. Select the **Authentication** method from the drop-down list to access the specified SQL instance. If you use the **SQL Server Authentication**, you are required to specify the **Username** and **Password.**
5. Click **Connect**. The database in the mirroring session will be loaded and displayed in the pane below.
6. You can perform the following actions on the listed databases in the mirroring session:
    - **Set Partner Off** – Select your desired database in the pane, and click **Set Partner Off** to cut off their mirroring sessions.
    - **Clean Up** – If you do not select the database, clicking **Clean up** will remove all of the configurations except the database, including the **Endpoint**, **Certificate**, **Login**, and **User**. If you select your desired databases in the pane, clicking **Clean up** will remove all of the configurations and the database.
        - **Drop master key** – If you select this option and click **Clean up**, the master key of this SQL instance will be removed.
        - **Only drop restoring database** – Select the desired database that you want to remove, and then click **Clean up** with this option selected**.** The selected database will be deleted and the configurations will be kept.

          ***Note**: If you do not select any database with this option selected to clean up, no databases or configurations will be removed.
7. After performing the actions provided (such as **Clean up** and **Set Partner Off**), a message pops up to inform you the job status and the local directory of the job report.
8. Click **Cancel** to exit this tool.

SP2010StorageUpgradeStub

This tool is used to report the detailed location information of the remaining DocAve 5 stubs checked by the Importing Stubs and BLOB Data or the Importing Connector Stub feature in Data Manager. For more detailed information about these two features, refer to DocAve 6 Control Panel Reference Guide.

Running the SP2010StorageUpgradeStub Tool

To run the SP2010StorageUpgradeStub tool, complete the following steps:

1. On the server where the DocAve Agent is installed, go to **Start** > **All Programs** > **Accessories** > **Command Prompt**.
2. Right-click **Command Prompt** and select **Run as administrator**. The **Command Prompt** interface appears.
3. Enter the command to access the Agent bin folder where the SP2010StorageUpgradeStub tool resides. It resides under *…\AvePoint\DocAve6\Agent\bin\SP2010StorageUpgradeStub.exe*.

   For example, enter **cd C:\Program Files\AvePoint\DocAve6\Agent\bin**.
4. Enter the following command to generate the report:

   ```
   SP2010StorageUpgradeStub.exe -WebApplicationUrl <Web Application URL> [-ContentDatabaseName <Content Database Name>]
   ```

   - **-WebApplicationUrl** – Enter the full URL of the Web application where the remaining DocAve 5 stubs reside.
   - **-ContentDatabaseName** – This parameter is optional. Enter the content database name under the specified Web application to only report the remaining DocAve 5 stubs' location information within this content database. If this parameter is not used, DocAve will check the remaining DocAve 5 stubs in all of the content databases under the specified Web application.

   For example, enter **SP2010StorageUpgradeStub.exe -WebApplicationUrl http://avepoint:1234** or enter **SP2010StorageUpgradeStub.exe -WebApplicationUrl http://avepoint:1234 -ContentDatabaseName AvePointDatabase01**.
5. After the command completes, the report will be saved under *…\AvePoint\DocAve6\Agent\jobs\D5StubCheckResult*. The report shows the type of the BLOB data, the URL of its SharePoint location, and the version of the file if that file has multiple versions (if the version is the current version of the file, it will leave the version field blank).

AgentToolSP2010(2013)MoveStub

The AgentToolSP2010(2013)MoveStub tool can be used for the following three purposes:

- **MoveSPSite** – Move one site collection from the original content database to another content database. Then move the stub information stored in the original stub database to the stub database configured for the destination content database.
- **MoveStub** – Move stub information stored in the original stub database to the stub database of the selected content database for the site collection.

  Use this command after you have moved a site collection to another content database using the Windows SharePoint 2010 (2013) Management Shell cmdlet **Move-SPSite**.
- **ChangeStubDB** – Change the stub database of the specified SharePoint objects and move all related stub information from the old stub database to the new stub database.

***Note**: We recommend you set the status of the source stub database's corresponding content database to read-only to avoid generating new stub information in the source stub database during the process of changing the stub database.

To change the content database's status to read-only, complete the following steps:

1. Open SQL Server Management Studio.
2. Expand the **Databases** node.
3. Double-click the source database.
4. Click **Properties** in the appeared drop-down list. The **Database Properties** window appears.
5. In the **State** field of the appeared window, select **Yes** from the drop-down list after **Database Read-Only**.
6. Click **OK** to save your changes.

After you finish using the tool, select **No** from the drop-down list after **Database Read-only** of the **State** field in SQL Server Management Studio.

Running the AgentToolSP2010(2013)MoveStub Tool

The AgentToolSP2010(2013)MoveStub tool directly accesses databases. As a result, only an account with sufficient permissions can be used to run the tool. Refer to the following for detailed information on the permissions required:

- Local System Permissions: Member of the local **Administrators** group.
- SharePoint Permissions:

- User is a member of the Farm Administrators group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
- Full Control to all zones of all Web applications via User Policy for Web Applications

- SQL Permissions:
  - Database Role of db_owner for all the databases related with SharePoint, including content databases, stub databases, SharePoint configuration database and Central Administration content database.
  - Database Role of dbcreator to the corresponding SQL Server, this permission is only required when you use the **ChangeStubDB** command and the entered new stub database does not exist on the specified SQL server.

Refer to the steps below to run this tool.

1. Navigate to …*AvePoint**DocAve6**Agent**bin* and locate **AgentToolSP2010MoveStub.exe** or **AgentToolSP2013MoveStub.exe**.
2. Double-click the tool to run it. A command-line interface (CLI) appears.
3. From within the CLI, enter a command applicable to you requirements:
   - –**MoveSPSite** – Enter this command to move one site collection from the original content database where it resides to another content database, and then move the stub information stored in the original stub database to the stub database configured for the destination content database. This is done so that all stubs can be accessed from SharePoint and operated in DocAve and SharePoint normally after the corresponding site collection is moved to the specified content database. Enter the –**MoveSPSite** command and press **Enter**. Then enter the following command according to the prompt message appears on the tool interface:

     -MoveSPSite [Site Collection URL] [DestinationDatabaseName] [SourceRBSProvider]<optional> [DestinationRbsProvider]<optional>

     Such as, **-MoveSPSite** http://avepoint/sites/docave DestinationStubDB, or **-MoveSPSite** http://avepoint/sites/docave DestinationStubDB **SP2010(2013)RBSProvider SP2010(2013)RBSProvider**

     - **Site Collection URL** – The complete URL of the site collection that you want to move to the specified content database.
     - **DestinationDatabaseName** – The name of the destination database that you want to move the specified site collection to.
     - **SourceRBSProvider (Optional)** – If the original content database where the specified site collection has RBS enabled and contains the stubs, enter the RBS Provider used by the original database here for keeping the stubs after moving them to the specified database. If not keeping the stubs after moving to the specified database, there is no need to enter the RBS Provider used by the

original database. Only **SP2010(2013)RBSProvider** can be entered here, and the value is case sensitive.

- **DestinationRbsProvider (Optional)** – If the destination content database where the specified site collection will be moved to has enabled RBS, enter the RBS Provider used by the destination database here. Only **SP2010(2013)RBSProvider** can be entered here and the value is case sensitive.

- –**MoveStub** – Enter this command to move the stub information stored in the original stub database to the stub database of the specified content database where the corresponding site collection resides. This action is done so that all of the old stubs can be accessed from SharePoint and operated in DocAve and SharePoint normally after the corresponding site collection is moved to a new content database. Enter the –**MoveStub** command and press **Enter**. Then, configure the following parameters according to the prompt messages that appear on the tool interface:

  - **Site Collection URL** – Enter the complete URL of the site collection that has been moved to another content database.
  - **Original Content Database Name** – Enter the name of the original content database where this site collection resided.

- –**ChangeStubDB** – Enter this command to change the stub database of the specified SharePoint objects and move all related stub information from the old stub database to the new stub database.. All of the old stubs can be accessed from SharePoint and operated in DocAve and SharePoint normally after the stub database of the corresponding SharePoint objects is changed. Enter the –**ChangeStubDB** command and press **Enter**. Then, configure the following parameters according to the prompt messages that appear on the tool interface:

  ***Note**: You must make sure the Control Service is started before running the tool.

  - **Change stub database mode** – Enter the mode used to change the stub database. Entering **0** changes the stub database without copying the existing data in the old stub database to the new one; entering **1** changes the stub database and then copies the existing data in the old stub database to the new one. A value of **1** is required if you wish for all of the old stubs to remain accessible and operational after changing the stub database.
  - **WebApplication URLs** – Enter the complete URL of the Web application where you want to change the content database's stub database. Multiple Web application URLs can be entered here when separated by spaces. An asterisk (*) represents all of the web applications in the specified farm. If you enter *, the stub database of all of the Web applications' content databases and the stub database of the selected Web application will be changed to the specified stub database.
  - **Content database names** – Enter the names of the content databases associated with the Web applications that you specified using the **Content database names** command. The stub databases of these content databases will be changed. Multiple names can be entered here when separated by spaces. An

asterisk (*) represents all of the content databases in the specified Web applications.

- **Destination SQL Server instance** – Enter the name/IP address of the SQL Server instance where the new stub database will reside.
- **SQL Server authentication mode** – Specify the authentication mode used to access the SQL Server instance. The value **0** represents **Windows Authentication** mode, and the value **1** represents **SQL Authentication** mode. If the **SQL Authentication** mode is used, you will be asked to enter the username and password used to access the SQL instance.

  ***Note:** If using the **Windows Authentication** mode, the user who runs the **AgentToolSP2010(2013)MoveStub** tool must have the **Database Creator** permission to log on the SQL server.

- **Stub database name** – Enter the name of the new stub database. If the specified stub database does not exist, it will be automatically created on the specified SQL Server instance when the move operation takes place.

  ***Note:** The database name is not case sensitive.

4. Once all of the necessary parameters have been configured, press **Enter** to run the command.
5. To exit the tool when finished, follow the instructions on the interface. You can also enter **exit** and press **Enter** to exit the tool. To continue using the tool, press any key (other than **Enter** or **Q**) to enter another command.

AgentToolSP2010eDiscoveryMapping & AgentToolSP2013eDiscoveryMapping

The AgentToolSP2010eDiscoveryMapping and AgentToolSP2013eDiscoveryMapping tools are used to map the crawl property to the managed property of a specified column, and save the property mapping to the Compliance database in order to enable the customized metadata filter rule in the advanced SharePoint search conditions.

***Note**: These tools support SharePoint 2010 and SharePoint 2013.

Permissions Requirements

To use the AgentToolSP2010eDiscoveryMapping and AgentToolSP2013eDiscoveryMapping tools properly, the user who uses these tools must have the following permissions:

- User is a member of the **Farm Administrators** group
- **Full Control** permission to the Search Service
- The **db_owner** database role in the Compliance Database

Running the AgentToolSP2010eDiscoveryMapping Tool or the AgentToolSP2013eDiscoveryMapping Tool

To run the AgentToolSP2010eDiscoveryMapping or AgentToolSP2013eDiscoveryMapping tool, complete the following steps:

1. Navigate to …*AvePoint**DocAve6**Agent**bin* and locate **AgentToolSP2010eDiscoveryMapping.exe** or **AgentToolSP2013eDiscoveryMapping.exe**.
2. Right-click on the tool and click **Run as administrator**. The AgentToolSP2010eDiscoveryMapping or AgentToolSP2013eDiscoveryMapping interface appears.
3. Configure the following settings in the AgentToolSP2010eDiscoveryMapping or AgentToolSP2013eDiscoveryMapping interface:
    a. Select a column: Refer to the steps below to locate the column that you want to map.
        - **Web Application** – Select a web application from the web application drop-down list. All of the site collections under the specified web application will be loaded in the site collection drop-down list for selection.
        - **Site Collection** – Select a site collection from the site collection drop-down list. All of the sites under the specified site collection will be loaded in the site drop-down list for selection.

- **Site** – Select a site from the site drop-down list. All of the site columns under the specified site will be loaded in the column title drop-down list for selection.
- **Column Title** – Select a column from the column title drop-down list.

b. Choose to map the current version's crawl property or the history version's crawl property for the selected column by checking the corresponding checkbox at the right corner of the interface.

c. Click **Enable** to start the mapping. The mapping status is displayed in the Colum Mapping field.

- **Yes** indicates that the corresponding crawl property of the specified column's current version or history version has been mapped successfully and saved in the Compliance database.
- **No** indicates that the corresponding crawl property of the specified column's current version or history version has not been mapped, or not saved in the Compliance database.

***Note**: A full crawl of the web application where the mapped column resides must be performed after running this tool to make the customized metadata filter rule effective.

AgentToolSP2010Connector Tool & AgentToolSP2013Connector Tool

The **AgentToolSP2010Connector** tool (for SharePoint 2010) or the **AgentToolSP2013Connector** (for SharePoint 2013) tool can update Connector document versions from DocAve 6.0 (including DocAve 6.0, 6.0.1 and 6.0.2) to DocAve 6 Service Pack 1 or later versions. The **AgentToolSP2010Connector** tool or the **AgentToolSP2013Connector** (for SharePoint 2013) tool provides the encrypted the password to connect to the file system before creating any Connector libraries using the **AgentToolSP2010ConnectorCreateList** tool. The **AgentToolSP2010Connector** tool or the **AgentToolSP2013Connector** (for SharePoint 2013) tool is also used to generate the report of the stub status of files and folders within specified scope.

Before using this tool, make sure that the BLOB Provider and the EBS/RBS settings are properly configured and that the Connector solutions are successfully deployed.

***Note**: The account used to run this tool must have the same permissions as the Agent Account. If the User Account Control is enabled, the **AgentToolSP2010Connector.exe** or **AgentToolSP2013Connector.exe** must run as Administrator.

Running the AgentToolSP2010Connector Tool or the AgentToolSP2013Connector Tool

By default, the **AgentToolSP2010Connector.exe** file or the **AgentToolSP2013Connector.exe** file is located in the Agent installation path: *…\AvePoint\DocAve6\Agent\bin.*

***Note:** All of the commands and parameters for this tool are not case-sensitive.

In the Command Line Interface, enter the command with the location of the **AgentToolSP2010Connector.exe** file (for SharePoint 2010) or the **AgentToolSP2013Connector.exe** file (for SharePoint 2013) as follows, and press **Enter**.

To get the help information of the **AgentToolSP2010Connector** tool or the **AgentToolSP2013Connector** tool, enter one of the following commands according to your SharePoint versions. After running this command, the command parameters and some examples are displayed in the Command Line Interface.

- `AgentToolSP2010Connector.exe -help` (this command is used for SharePoint 2010)
- `AgentToolSP2013Connector.exe -help` (this command is used for SharePoint 2013)

For more information on each specific operation, enter the following commands according to your SharePoint versions to get the detailed help information.

- `AgentToolSP2010Connector.exe –help <operation>` (this command is used for SharePoint 2010)
- `AgentToolSP2013Connector.exe –help <operation>` (this command is used for SharePoint 2013)

***Note:** All of the operations in the following sections are referred to the tool for SharePoint 2010. If you are using SharePoint 2013, replace **AgentToolSP2010Connector.exe** by **AgentToolSP2013Connector.exe**, all of the other parameters keep the same.

Click the following links to jump to the corresponding operation sections.

- Operation -o UpgradeVersion
- Operation -o EncryptPassword
- Operation -o ReportItems
- Operation -o UpgradeConnectedLibrary (SharePoint 2013 Only)

Operation -o UpgradeVersion

This operation is used to update the document versions in all Connector libraries in the SharePoint farm from DocAve 6.0 (including DocAve 6, DocAve 6 CU1, and DocAve 6 CU2) to DocAve 6 Service Pack 1 or later versions.

For documents that reside in Connector libraries, the real files of the document versions are stored in a hidden folder named **.fsdl** in the connected storage path. The **AgentToolSP2010Connector** tool (for SharePoint 2010) or the **AgentToolSP2013Connector** tool (for SharePoint 2013) only upgrades the real files of the document versions, but does not upgrade the version links in Connector libraries.

If the documents stored in your Connector libraries have history versions, you must run this tool to upgrade document versions because the following changes are made to the stub database of DocAve 6 Service Pack 1 and later versions.

Before DocAve 6 Service Pack 1 (and later versions), one document version in the storage path may have several records in the stub database. However, from DocAve 6 Service Pack 1 on, one document version in the storage path can only have one record in the stub database.

This tool makes copies of the document versions in the storage path, and makes sure the relationship between the document version and the stub database record is a one-to-one mapping.

After the upgrade from DocAve 6.0 to DocAve 6 Service Pack 1 or later versions, you will then be able to open the old document versions successfully.

If the documents stored in your Connector libraries do not have any history versions, there is no need to run this tool.

Syntax

```
AgentToolSP2010Connector.exe
```

-o UpgradeVersion

```
[-url <The URL of the node where the document versions you want to update>]
```

Parameters

Parameter	Required?	Value and Description
-url	Optional	Enter the absolute URL of the supported SharePoint scopes: Web applications, site collections, sites, or libraries. If this is done, only the document versions of the Connector libraries within the specified scope will be updated. ***Note**: Quote the parameter value with double quotation marks if there are spaces in the parameter value.

Examples

```
AgentToolSP2010Connector.exe –o UpgradeVersion
```

Or

```
AgentToolSP2010Connector.exe –o UpgradeVersion –url http://server/site
```

Checking the Job Status

After running the upgrade job using this tool, you can check the job status in the Summary Report and Detail Report that are generated in the Agent installation path, which is *…\AvePoint\DocAve6\Agent\Logs\Connector* by default.

If there are some versions/libraries that the tool failed to upgrade, you can check the detailed reasons in the Detail Report.

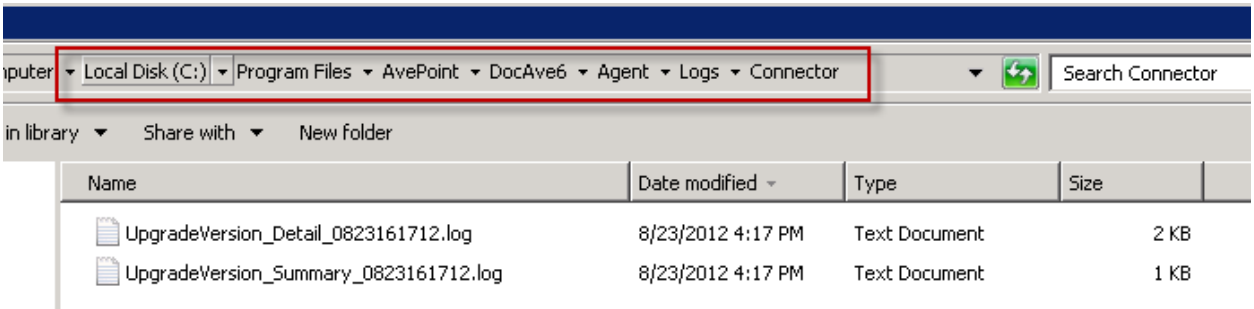


Figure 13: Job reports.

Operation -o EncryptPassword

This operation is used to encrypt the password for the AgentToolSP2010ConnectorCreateList tool and the AgentToolSP2013ConnectorCreateList tool.

Syntax

```
AgentToolSP2010Connector.exe

-o EncryptPassword
```

After running this command, enter the password that you want to encrypt, and then enter this password again for confirmation. The encrypted password will be displayed under the **The string below is your password after being encrypted** prompt.

Operation -o ReportItems

This operation is used to generate the report of the stub status of files and folders within specified scope.

The generated report will be saved in the following path: *…\AvePoint\DocAve6\Agent\Logs\Connector*. Each job will generate a folder named in the format of **ReportItems_DateTime** under this directory. In this folder, there may be three types of reports which depend on parameters included in the job.

- Summary Report – Includes stub status and basic information for all of the libraries checked under the specified scope.
- SharePoint Report– Includes stub status and other basic information for all of the files and folders in the library under the specified scope. Each library under the specified scope will generate one SharePoint report. The report is named in the following format: **ListURL(SP).csv**. If the **–includeVersion** parameter is used, each version of file together with its stub status will be displayed as an entry in the SharePoint report.
- Storage Report – Includes the basic information for all of the files and folder in the storage path configured for the library. Every library configured a storage path will generate one storage report. The report is named in the following format: **ListURL(Storage).csv**. This report can be only generated when you use the **–includeStorage** parameter.

Syntax

```
AgentToolSP2010Connector.exe

-o ReportItems

[-url <The URL of the node where the files and folders' report you want to get>]

[-includeStorage>]

[-includeVersion]
```

Parameters

Parameter	Required?	Value and Description
-url	Optional	Enter the absolute URL of the supported SharePoint scopes: Web applications, site collections, sites, or libraries. If this is done, only files and folders of Connector libraries within the specified scope will be reported. ***Note**: Quote the parameter value with double quotation marks if there are spaces in the parameter value.
-includeStorage	Optional	This parameter is used to generate the storage report, which contains all of the files and folders information in the storage path configured for the Connector library.
-includeVersion	Optional	This parameter is used to include history versions of the files and folders within the specified scope in the SharePoint report.

Examples

```
AgentToolSP2010Connector.exe –o ReportItems –url http://server/site
```

Or

```
AgentToolSP2010Connector.exe –o ReportItems –url http://server/site -includeStorage
```

Or

```
AgentToolSP2010Connector.exe –o ReportItems –url http://server/site -includeStorage -
includeVersion
```

Operation -o UpgradeConnectedLibrary (SharePoint 2013 Only)

After you have updated Connector from a SharePoint 2010 to SharePoint 2013 environment with connected libraries, you must run the command UpgradeConnectedLibrary for the **AgentToolSP2013Connector** tool to make these connected libraries available before you use these connected libraries in SharePoint 2013. The basic function of this new command for

AgentToolSP2013Connector Tool is to update the Connector EventHandler to the Version of SharePoint 2013, and to update the List Image URL of Connector libraries.

After running the update job using this tool, check the job status in the Reports that are generated in the Agent installation path, which is **…\AvePoint\DocAve6\Agent\Logs\Connector** by default. If there are some libraries that the tool failed to update, check the detailed reasons in the Report or in the Log file. You can re-run the job according to the prompt information in the Log file.

Perquisites for Running This Operation

The prerequisites for using this new command are:

- DocAve 6 SP2 or a later version is used in your SharePoint 2010 environment.
- After mounting the database with Connector to the farm of SharePoint 2013 from SharePoint 2010 environment, you have updated the site style to the SharePoint 2013 site style.
- The Connector solutions for SharePoint 2013(SP2013ConnectorContentLibrary.wsp and SP2013ConnectorMediaLibrary.wsp) must have been deployed to your SharePoint 2013 farm.
- The DocAve agents in SharePoint 2010 and SharePoint 2013 point to the same DocAve Manager.

Syntax

```
AgentToolSP2013Connector.exe

-o UpgradeConnectedLibrary

[-url <The URL of the node where the libraries you want to update>]
```

Parameters

Parameter	Required?	Value and Description
-url	Optional	Enter the absolute URL of the supported SharePoint scopes: Web application, site collections, sites, or libraries. ***Note**: Quote the parameter value with double quotation marks if there are spaces in the parameter value.

Examples

```
AgentToolSP2013Connector.exe -o UpgradeConnectedLibrary
```

Or

```
AgentToolSP2010Connector.exe –o UpgradeConnectedLibrary –url http://server/site
```

AgentToolSP2010OrphanStubClean & AgentToolSP2013OrphanStubClean

The **AgentToolSP2010OrphanStubClean** and **AgentToolSP2013OrphanStubClean** tools are used to search for and clean up orphan stubs that exist in the SharePoint 2010 or SharePoint 2013 environment.

Orphan stubs are stubs whose real content have been deleted or stubs that are not able to connect to their real content.

You can perform the following two functions using this tool:

- Search for orphan stubs in your SharePoint 2010 or SharePoint 2013 environment and generate an Orphan Stub report for your environment.
- Clean up orphan stubs according to the orphan stub report generated in the function above.

***Note**: The account used to run this tool must have the same permissions as the Agent Account.

Searching for the Orphan Stubs

To search for orphan stubs in your SharePoint environment, complete the following steps:

1. By default, the **AgentToolSP2010OrphanStubClean.exe** or **AgentToolSP2013OrphanStubClean.exe** file is located in the Agent installation path: *…\AvePoint\DocAve6\Agent\bin.* Navigate to this location.
2. Double-click the **AgentToolSP2010OrphanStubClean.exe** or **AgentToolSP2013OrphanStubClean.exe** file to run this tool.
3. Input the following commands to search for the orphan stubs in your SharePoint environment and generate the orphan stub report:
    - Use the **RBSOrphanCleanUp** command if you enabled RBS for your environment in order to use DocAve Storage Optimization modules.

      RBSOrphanCleanUp -WebApp http://hostname/ **-ContentDB** WSS_Content **-SiteCollection** http://hostname/sites/test **-Action** Report **-File** C:\OrphanStubReport.csv **-AfterTime** 2012-1-1

    - Use the **EBSOrphanCleanUp** command (only used for searching for orphan stubs in SharePoint 2010) if you enabled EBS for the farm in order to use DocAve Storage Optimization modules.

      EBSOrphanCleanUp -WebApp http://hostname/ **-ContentDB** WSS Content **-SiteCollection** http://hostname/sites/test **-Action** Report **-File** C:\OrphanStubReport.csv **-AfterTime** 2012-1-1

This table below contains detailed information on each of the parameters:

Parameter	Type	Description
-WebApp	Required	The URL of the Web application where you want to search for or delete the orphan stubs.
-ContentDB	Optional	The name of the content database where the orphan stubs reside. This is an optional parameter. If you use this parameter, only the specified content database is searched. If you do not use this parameter, the entire Web application is searched.
-SiteCollection	Optional	The URL of the site collection where you want to search for or delete the orphan stubs. This is an optional parameter. If you use this parameter, only the specified site collection is searched. If you do not use this parameter, the entire Web application is searched.
-Action	Required	This action generates an orphan stub report that displays the orphan stubs discovered by this command. The value of this parameter is **Report**.
-File	Required	The full path where you want to save the orphan stub report. The path must be detailed to the name of the report file. For example, *C:\OrphanStubReport.csv*. The report file is generated automatically if it does not exist. If there is already a file with the same name existing in the specified location, the newly generated report file will overwrite the existing one. ***Note**: This command only supports generation of report files in .csv format.
-AfterTime	Required	Only the orphan stubs generated after the specified date searched for. The date must be in the format of *YYYY-MM-DD*. **Y** stands for year, **M** stands for month, and **D** stands for day.

4. Press **Enter** to run the tool.
5. After the search job completes, you can check the orphan stub report under the location specified in the command.

Cleaning up the Orphan Stubs

To clean up the orphan stubs discovered in the Searching for the Orphan Stubs section, complete the following steps:

1. Enter the following Command to clean up the EBS or RBS orphan stubs:
    - For cleaning up the EBS orphan stubs, enter the command like **EBSOrphanCleanUp -Action** *Clean* -**File** *C:\OrphanStubReport.csv*.
    - For cleaning up the RBS orphan stubs, enter the command like **RBSOrphanCleanUp -Action** *Clean* -**File** *C:\OrphanStubReport.csv*.
2. This table contains the detailed information for each of the parameters:

Parameter	Type	Description
-Action	Required	This action is used to clean up the orphan stubs. The value of this parameter is **Clean**.
-File	Required	The full path where the orphan stub report resides. The path must be detailed to the name of the report file. For example, *C:\OrphanStubReport.csv*.

3. Press **Enter** to run the tool. After the job completes, the orphan stubs recorded in the specified orphan stub report are deleted from your SharePoint environment.

Replicator Analyzer Tool

Use the Replicator Analyzer tool to delete failed jobs' Profile Settings configuration from the DocAve6_ReplicatorDatabase and modify the SP2010Replicator.xml configuration file in bulk.

For SharePoint 2010 environments, use the SP2010ReplicatorAnalyzer tool. For SharePoint 2013 environments, use the SP2013ReplicatorAnalyzer tool.

By default, the **SP2010ReplicatorAnalyzer.exe** file and the **SP2013ReplicatorAnalyzer.exe** file are located in the Agent installation path: *…\AvePoint\DocAve6\Agent\bin*.

Deleting Failed Job's Profile Settings Configuration

The Replicator Analyzer tool deletes failed jobs' Profile Settings configuration from the DocAve6_ReplicatorDatabase. After deleting the Profile Settings configuration, incremental replication can be performed successfully.

Regardless of whether a Replicator job has finished or failed, Profile Setting mappings are generated in the DocAve6_ReplicatorDatabase during the job process. When performing an incremental replication after a failed replication job, the Profile Settings configurations of this incremental replication are compared with the Profile Settings configuration of the former failed replication. Since all settings, content types, columns, and other configurations are the same this incremental replication is skipped and the contents are not replicated. However, the corresponding contents do not exist in the destination since the former job failed. This tool is used to delete the useless Profile Settings configuration from failed jobs, thus ensuring that the incremental replication completes successfully.

To delete a failed job's Profile Settings configuration, run the tool by completing the following steps:

1. Use a DocAve Agent Account to run this tool. Right-click **SP2010ReplicatorAnalyzer.exe/SP2013ReplicatorAnalyzer.exe** file, and select **Run as Administrator**.
2. In the Command Line Interface, enter the command to browse to the **SP2010ReplicatorAnalyzer.exe/SP2013ReplicatorAnalyzer.exe** file, and press **Enter**.

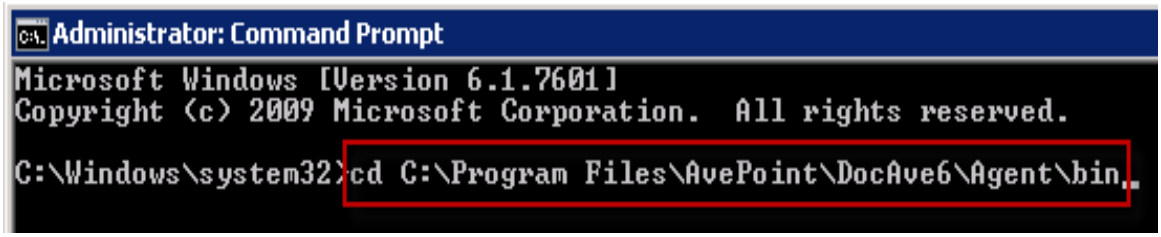


Figure 14: Location of the Replicator Analyzer Tool.

3. Enter the following command to delete the configuration according to the specified condition. The format of the command is **SP2010ReplicatorAnalyzer** (or **SP2013ReplicatorAnalyzer**)**–type**

CMD –data DeleteDirtyDesign –mappingid [MappingID] –itemid [ItemID] –designType [DesignType]

- **SP2010ReplicatorAnalyzer** (or **SP2013ReplicatorAnalyzer**) – Execute the **Replicator Analyzer** tool.
- **-type CMD** – Run the tool by CMD command.
- **-data DeleteDirtyDesign** – Enable the delete function.
- **-mappingid[MappingID]** – Get configuration according to specified Mapping ID. **[MappingID]** is required to be entered. The following steps describe how to find the Mapping ID of your desired job.
    - In DocAve Manager, click **Job Monitor** to enter the interface.
    - In the Job Monitor interface, select your desired job, and then click **View Mappings** on the ribbon. The View Mappings tab appears.
    - In the **Job ID** column, the character strings after _ is the Mapping ID. For example, the Job ID is **RP20120830041514729574_2db64471-d275-4746-88c4-89d17bec612a**. The Mapping ID is **2db64471-d275-4746-88c4-89d17bec612a.**
- **-itemid[ItemID]** (Optional) – Filter configuration according to specified Item ID. Item ID is the ID of a SharePoint object and it can be found in SharePoint Content Database.
- **-designType[DesignType]** (Optional)– Further filter configuration according to specified Design Type. Design Type is the type of configuration. It is strongly recommended contacting with our technical staff to help you gain Design Type if you need to delete configuration of a specified Design Type in a Mapping.

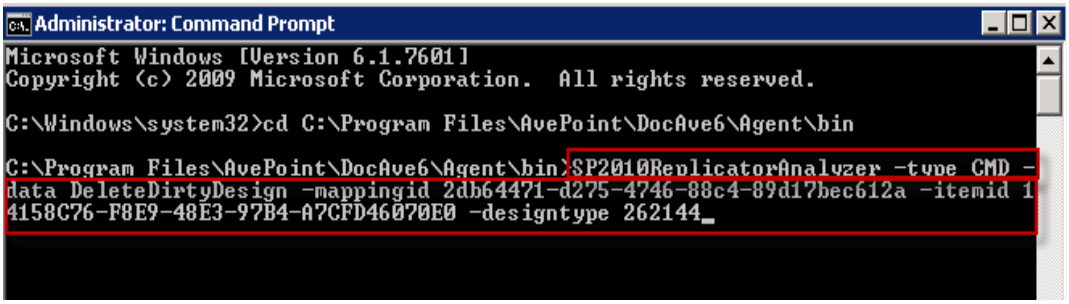


Figure 15: Example of running the Replicator Analyzer Tool.

***Note:** If you only set Mapping ID as the condition, enter the command like the following example: *SP2010ReplicatorAnalyzer (or SP2013ReplicatorAnalyzer) –type CMD –data DeleteDirtyDesign –mappingid 2db64471-d275-4746-88c4-89d17bec612a*.

4. Press **Enter** to run the tool and delete the failed job's configuration.

Modifying the Configuration Files in Bulk

The Replicator Analyzer tool helps you to modify the SP2010Replicator.xml configuration files in bulk.

To modify the configuration files in bulk, run the tool by completing the following steps:

1. Use a DocAve Agent Account to run this tool. Right-click **SP2010ReplicatorAnalyzer.exe** file or **SP2013ReplicatorAnalyzer.exe** file, and select **Run as Administrator**.
2. In the Command Line Interface, enter the command to browse to the **SP2010ReplicatorAnalyzer.exe** file or **SP2013ReplicatorAnalyzer.exe** file, and press **Enter**.

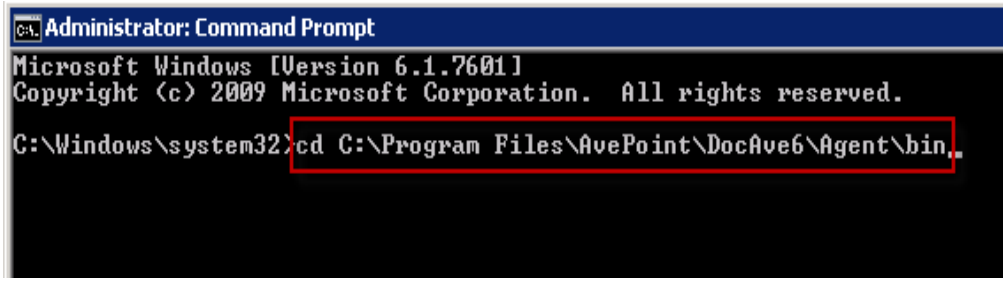


Figure 16: Location of the Replicator Analyzer Tool.

3. Enter the following command to modify the configuration file. The format of the command is **SP2010ReplicatorAnalyzer** (or **SP2013ReplicatorAnalyzer**) **–type CMD –data ModifyConfigurationFile –scope [Agent|AgentGroup|Farm|All] –scopeId [AgentHost|AgentGroupName|FarmId] –path –modifytype [Add|Delete|Modify] –value**
    - SP2010ReplicatorAnalyzer (or SP2013ReplicatorAnalyzer) – Execute the Replicator Analyzer tool.
    - **-type CMD** – Run the tool by CMD command.
    - -**data ModifyConfigurationFile** – Replicator Analyzer tool will modify the configuration file.
    - -**scope [Agent|AgentGroup|Farm|All]** – The scope of the configuration file that you are about to modify. A DocAve agent, an agent group, a farm, or all of the DocAve Agents that register to DocAve Manager.
    - - **scopeId [AgentHost|AgentGroupName|FarmId]** – The ID of your selected scope. The Agent Host of the DocAve Agent, the agent group name, or the farm ID.

      ***Note**: If the parameter of **scope** is **All**, here you do not need to enter the scope ID.
    - - **path** – The path of the element in the configuration file.

      ***Note:** The entered path is case sensitive.

        - Modify the attribute of an element – For example, if you want to modify the attribute “IsDeleteDefaultList” of the element “ScheduleConfiguration”, the parameter of path is “Configuration/ReplicatorConfig/ScheduleConfiguration”.
        - Add an element – For example, if you want to add an element under “NonReplicationLists”, the parameter of path is “Configuration/ReplicatorConfig/FilterConfiguration/NonReplicationLists”.

- Delete an element – For example, if you want to delete an element from “NonReplicationLists”, the parameter of path is “Configuration/ReplicatorConfig/FilterConfiguration/NonReplicationLists”.

- **-modifytype [Add|Delete|Modify]** – Add, delete, or modify an element.
- -**value** – The value of the element.
  - Modify the attribute – “value”.

    For example, **-value “IsDeleteDefaultList:True”**.

  - Add an element with single attribute – “type:typeName;innertext:attribute value”.

    For example, **-value “type:List;innertext:list1”**.

  - Add an element with multiple attributes – “type:typeName;attribute1: attribute 1 value;attribute2:attributea value”.

    For example, **-value “type:List;Name:list1;Template:template1”**.

  - Delete an element with single attribute – “innertext:attribute value”.

    For example, **-value “innertext:list1”**.

  - Delete an element with multiple attributes – “attribute1:attribute1;attribute2:attribute2 value”.

    For example, **-value”Name:list1;Template:template1”**.

***Note**: The entered attribute name and attribute value are case sensitive.

AgentToolDataTransferGUI

The Data Transfer Service Tool is used to check the newly added and modified data in the source export location and transfer the new data to the destination export location. Then the import job is triggered automatically and the new data is imported to the destination node. The Data Transfer Service Tool is integrated with Replicator's differential compression function.

In order to use the differential compression function, Remote Differential Compression must be configured in your operating system on the servers where the source and destination DocAve Agents are installed.

System Requirements

Refer to the following information to configure the Remote Differential Compression for your DocAve Agent servers. For the Windows Server 2003 operating system, Remote Differential Compression MSI must be configured first:

1. Navigate to the following locations to download the installation file of Remote Differential Compression MSI according to the version of your operating system:

   http://download.microsoft.com/download/e/e/0/ee02f60b-c002-47f7-a92b-8d7a58561cd9/AMD64FRE/msrdcoob.exe(For the processers except the IA64 processer)

   http://download.microsoft.com/download/e/e/0/ee02f60b-c002-47f7-a92b-8d7a58561cd9/IA64FRE/msrdcoob.exe (Only for IA64 processer)

   http://download.microsoft.com/download/e/e/0/ee02f60b-c002-47f7-a92b-8d7a58561cd9/X86FRE/msrdcoob.exe(Only for X86 operating system)

2. After downloading the specified installation file of Remote Differential Compression MSI, double-click the downloaded file.
3. Select the **I Agree** option to agree with the license agreement.
4. Click **Next** on the Software Update Installation Wizard and finish the installation.

For the Windows Server 2008 operating system, complete the following steps to install the Remote Differential Compression feature:

1. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Features Summary** > **Add Features**.
2. Select the checkbox in front of the **Remote Differential Compression** feature in the pop-up window.
3. Click **Install** to install it.

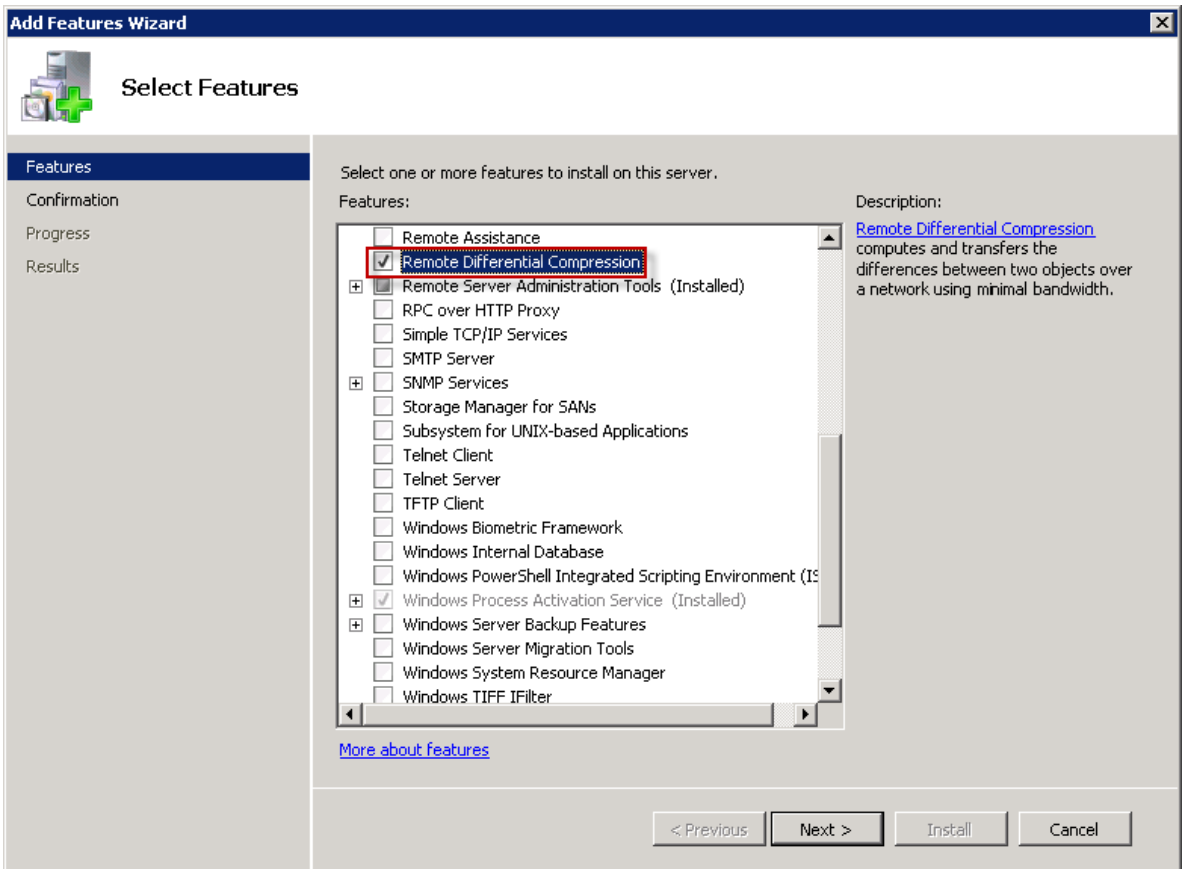


Figure 17: Remote Differential Compression in Windows Server 2008 operating system.

For the Windows Server 2012 operating system, complete the following steps to install the Remote Differential Compression feature:

1. Navigate to **Start** > **Administrative Tools** > **Server Manager** > **Local Server/All Servers** > **ROLES AND FEATURES**.
2. Click **TASKS** and select **Add Roles and Features**.
3. In the **Features** section, select the checkbox in front of the **Remote Differential Compression** feature.
4. Click **Install** to install it.

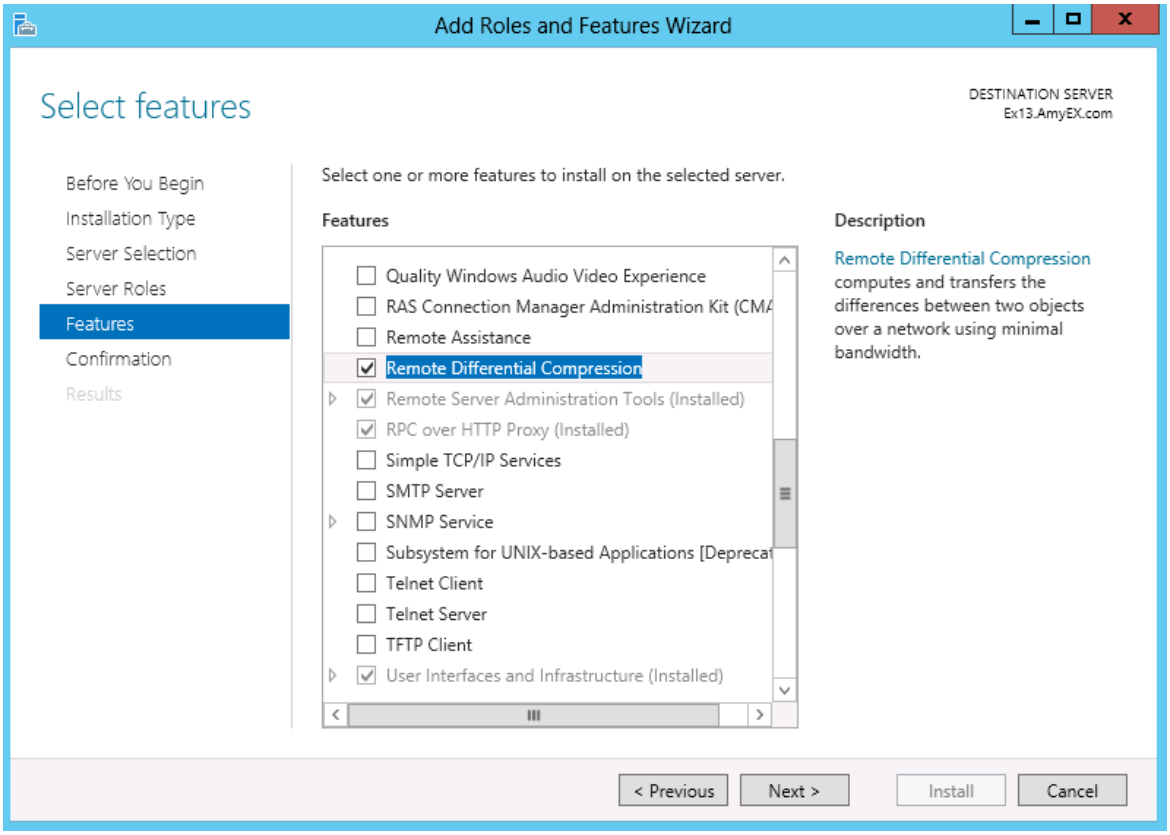


Figure 18: Remote Differential Compression in Windows Server 2012 operating system.

Enabling Differential Compression

To use the Data Transfer Service Tool, you must enable differential compression first by completing the following steps:

1. In DocAve Manager, navigate to **Administration** > **Replicator** > **Profile Settings** > **Export Profile**. In the **Advanced Options** sub-profile, select the **Differential data compression** checkbox. After configuring other settings, save this main profile.
2. In the **Home** tab, enable **Data Export**, then select your desired source node and a previously configured source export location.
3. Select the previously configured main profile and click **Add to Queue**.
4. Click **Save As a Plan** to create a replication plan and then run an offline replication job to export the data to the source export location.

Configuring Data Transfer Service Tool

To configure the Data Transfer Service Tool, complete the following steps:

1. On the servers where the source and destination DocAve Agent are installed, create an INI file named **AgentToolDataTransfer** in the path where the **AgentToolDataTransferGUI.exe** resides respectively. By default, the **AgentToolDataTransferGUI.exe** is located in the Agent installation path: *…\AvePoint\DocAve6\Agent\bin*.
2. In the source **AgentToolDataTransfer.ini** file, configure the following information.
    - host: Control Service Host
    - port: Control Service Port
    - user: The user who can log in Control Service
    - plan: The import plan name

      ***Note**: Only one plan is supported.

    - enablessl: Enable SSL or not.

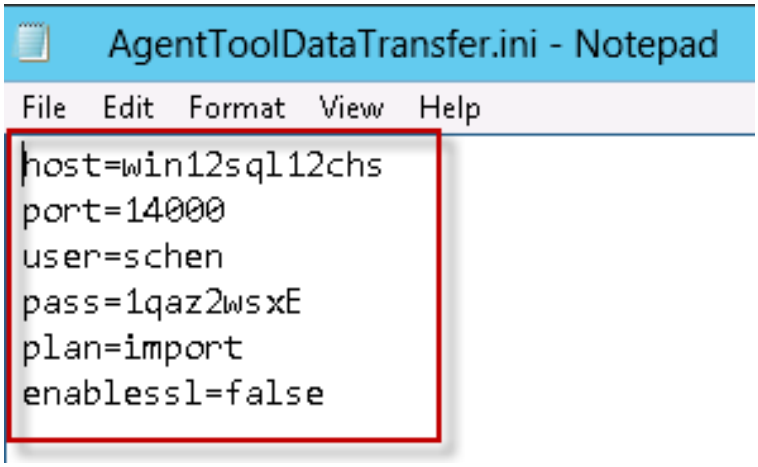


Figure 19: The source AgentToolDataTransfer.ini file.

3. In the destination **AgentToolDataTransfer.ini** file, enter the path of **Cmdlet.dll** file: *…\AvePoint\DocAve6\Shell\DocAveModules\DocAveModule\Cmdlet.dll*.

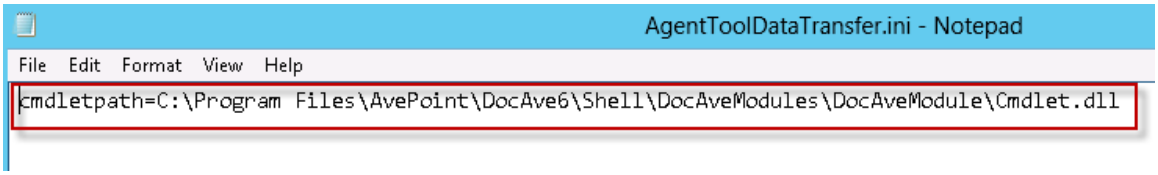


Figure 20: The destination AgentToolDataTransfer.ini file.

4. On the server where the destination DocAve Agent is installed, navigate to *…\AvePoint\DocAve6\Agent\bin*. Find the **AgentToolDataTransferGUI.exe** file and right-click it to select **Run as administrator**.

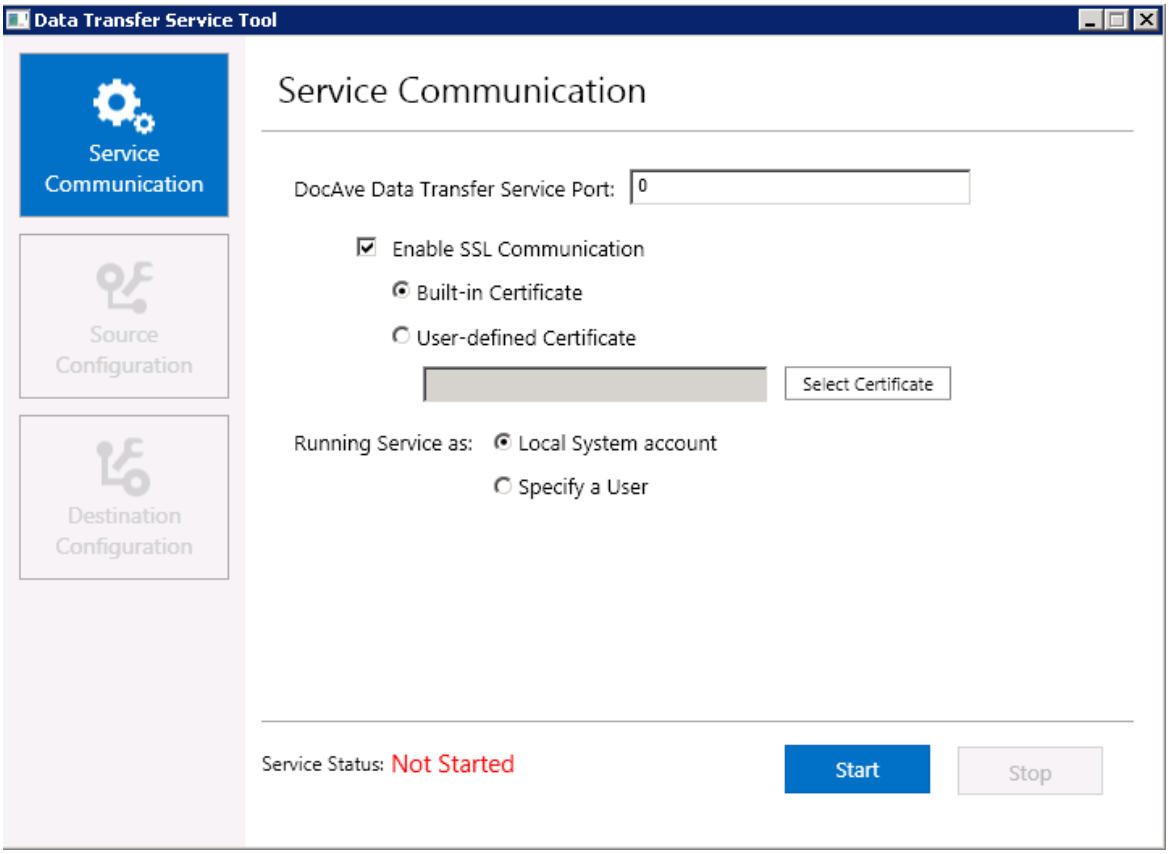


Figure 21: The Data Transfer Service Tool interface.

a. In **Service Communication**, complete the following configurations:

- **DocAve Data Transfer Service Port** – Enter the service port in the text box.
- **Enable SSL Communication** – Select this option to enable the secure encrypted transmission of data and then select the certificate.
  - **Built-in Certificate** – Use the built-in certificate.
  - **User-defined Certificate** – Click **Select Certificate** to select your desired certificate.
- Select running service as **Local System account** or specify a user to run the service.
- Click **Start** to start the service.

  ***Note**: If you choose **Specify a User** to run the service, the **Set Service Login** window pops up. Enter the username and password in the corresponding text boxes. The user requires at least read/write permission to the destination export location.

b. Click **Destination Configuration** and enter the destination export location which is configured in DocAve Manager. Click **Apply** to apply the destination configuration settings.

5. In the server where the source DocAve Agent is installed, navigate to …*AvePoint**DocAve6**Agent**bin*. Find the **AgentToolDataTransferGUI.exe** file and right-click it to select **Run as administrator**.

    a. In **Service Communication**, complete the following configurations:

        - **DocAve Data Transfer Service Port** – Enter the service port in the text box.
        - **Enable SSL Communication** – Select this option to enable the secure encrypted transmission of data and then select the certificate.
            - **Built-in Certificate** – Use the built-in certificate.
            - **User-defined Certificate** – Click **Select Certificate** to select your desired certificate.
        - Select running service as **Local System account** or specify a user to run the service.
        - Click **Start** to start the service.

          ***Note**: If you choose **Specify a User** to run the service, the **Set Service Login** window pops up. Enter the username and password in the corresponding text boxes. The user requires at least read/write permission to the destination export location.

    b. Click **Source Configuration** and enter the **Source Location**, **Destination Host**, and **Destination Port** in the corresponding textbox. Click **Validation Test** to test the communication. Then click **Apply** to apply the source configuration settings.

6. The source data will be transferred to the destination export location.

***Note**: If you want to configure the Data Transfer Service Tool on the servers where no DocAve Agents are installed, copy the **AgentToolDataTransfer.exe** file, the **AgentToolDataTransferGUI.exe** file, and the **DocAveModules** folder to your desired path. If so, the path of **Cmdlet.dll** file entered in the destination **AgentToolDataTransfer.ini** file is …*DocAveModules**DocAveModule**Cmdlet.dll*. By default, the **AgentToolDataTransfer.exe** file and the **AgentToolDataTransferGUI.exe** file are in …*AvePoint**DocAve6**Agent**bin* of the server where DocAve Agent is installed. The **DocAveModules** folder is in …*AvePoint**DocAve6**Shell* of the server where DocAve Agent is installed.

Triggering Import Automatically

To automatically trigger an import, complete the following steps:

1. In DocAve Manager, create a Replicator import plan.

   ***Note**: The plan name must be the same as the one you configured in the INI file.

2. Run an import job to test whether the data can be imported properly.
3. When new data is added in the source, run an export job and the import job will be triggered. The exported data will be replicated to the destination location.

DocAve URL Convert Tool

This tool allows you to convert any URLs to the specified ones in the selected scope (Web Application, Site Collection, Site, or List).

***Note**: When converting the URL in the document content for SharePoint 2013, some properties of the document will be changed at the same time. For example, the modified time of the document will be updated.

Required Permissions

To use DocAve URL Convert Tool properly, make sure the user has enough permissions.

Local System permission:

- User is a member of the local **Administrators** group.

SharePoint permissions:

- User is a member of the Farm **Administrators** group. Since Administrator works across farms and on all SharePoint settings and configurations, this account is needed in order to provide the best and most complete quality of service.
- Policy for Web Application: Full Control
- User Profile Service Application permissions:
    - Create Personal Site (required for personal storage, newsfeed, and followed content)
    - Follow People and Edit Profile
    - Use Tags and Notes
    - Full Control
- Managed Metadata Service: Term Store Administrator
- Business Data Connectivity Service: Full Control
- Search Service: Full Control

SQL permission:

- Database Role of **db_owner** for all the databases related with SharePoint, including Content Databases, Configuration Database, and Central Admin Database.

How to Use This Tool

To use the DocAve URL Convert tool, complete the following steps:

1. Navigate to …*Program Files**AvePoint**DocAve6**Agent**bin* in the machine where the DocAve Agent is installed.

2. Run the **AgentToolSP2010ConvertURL.exe**/**AgentToolSP2013ConvertURL.exe** found in the bin folder according to your SharePoint. The **DocAve URL Convert Tool** interface appears.
3. Select the **Level** of the URLs you want to convert from the **Level** drop-down list. Four levels are available: **Web Application**, **Site Collection**, **Site**, and **List**.
4. Enter the URL of the specified level where you want to change the links in the **Scope URL** field.
5. Two URL converting modes are available: **Single Mapping** and **Bulk Mapping**.

   Single Mapping enables to you to convert the selected URL to another one in the specified scope; **Bulk Mapping** enables you to convert the selected URLs to the corresponding ones in bulk in the specified scope.

   a. **Single Mapping** – Click the **Single Mapping** radio button to enable the Single Mapping.

      - Enter the URL that you want to convert in the **Find URL** field.
      - Enter the URL that the specified URL will be converted to in the **Replace with URL** field.

   b. **Bulk Mapping** – Click the **Bulk Mapping** radio button to enable the Bulk Mapping.

      - Click **Upload** to upload the previously created xml file that contains URL mappings. For more information about creating an xml file, refer to the Creating the XML File section.

6. After configuring the URL replacing settings, you can Click **Option>>** to configure the advanced settings if necessary. The specified URLs will be converted using the default advanced settings if you do not change it.

   To configure the advanced settings, complete the following steps:

   a. **Conversion Options** – Two options are available: **Case-Sensitive** and **Replace Relative URL**.

      - **Case-Sensitive** – The URLs you entered are case sensitive with this option selected.
      - **Replace Relative URL** – Only the relative URL of the specified URL will be replaced with this option selected. For example, set the value of **Find URL** as **http://AvePoint2/sites/siteB** and the value of **Replace with URL** as **http://AvePoint/sites/siteA**. With this option selected, the URL **http://AvePoint2/sites/siteB** will be changed to **http://AvePoint2/sites/siteA** after converting. If this option is not selected, the URL will be changed to **http://AvePoint/sites/siteA** after converting.

   b. **Object Level** – You can also convert the specified URLs to the corresponding ones in the following scopes by selecting the corresponding checkbox. By default, the URLs will not be changed in these scopes if the corresponding checkboxes are not selected.

      - **Item** – Replace the URL if it exists in the item's properties.

        ***Note**: This option works only when the **Single Mapping** mode is selected.

- **Web Part** – Replace the URLs that locate in the following types of Web parts in customized pages: **Content Editor** Web part, **Image Viewer** Web part, and the **Page Viewer** Web part.
- **Article Page** – Replace the URL for the properties (Page Content and Page Image) of Article Page in the **Pages** list.
- **Document** – Replace the URL that exists in the Word or Excel in the document library including the uploaded Word or Excel.

  ***Note**: This option works only on the machine that has Office 2007/2010/2013 installed.

c. **Report Location** – Click **Modify** to select a location to store the job reports. By default, the location is the desktop.

7. You can click **Test Run** to simulate the URL converting as you configured, or click **Replace** to start converting the URLs as you have defined above. After clicking **Test Run** or **Replace**, a **Detail Report** will be generated in the specified report location, and an **Error Report** will be generated only when errors occurred during the URL converting. You can view the URL replacing details in the corresponding job report.
8. Click **Exit** to exit this tool.

Creating the XML File

Create an xml file as the screenshot below for Bulk Mapping mode. Change the values of the **Mapping find** attribute and the **replaceWith** attribute to the URLs you want to convert and to be converted to respectively.

```
<MappingPairs>
  <Mapping find="http://AvePoint/sites/siteA" replaceWith="http://AvePoint/sites/siteB" />
  <Mapping find="/TestLink1" replaceWith="/TestLink2" />
  <Mapping find="/link1/link2" replaceWith="/link3/link4" />
  <Mapping find="link1" replaceWith="link5" />
</MappingPairs>
```

Figure 22: The xml file for the DocAve URL Convert Tool.

To create an xml file, complete the following steps:

1. Create a txt document.
2. Enter a **MappingPairs** node in the created txt document.
3. Enter the **Mapping find** and **replace with** attributes under this node.
   - **Mapping find** – Enter the URL that you want to convert.
   - **replaceWith** – Enter the URL that you want the specified URL to be converted to.

   Enter more groups of mapping attributes to add more mappings.

4. Save this txt document in the xml format after setting up the URL replacing mappings.

***Note**: If you set up several replaced policies for one URL, only the deepest URL can be replaced. Take the mapping XML file above as an example. After running the tool, the URL **http://avepoint/sites/TestSite/link1/link2** will be changed to **http://avepoint/sites/TestSite/link3/link4** other than **http://avepoint/sites/TestSite/link5/link2**.

DocAve Migrator Tool

The DocAve Migrator Tool is mainly designed to scan the source data for migration, generate the scan report for your reference, and set up security mapping that can be used when performing a DocAve migration job.

You can use the Migrator Tool to scan source data from Lotus Notes, Quickr, eRoom, File System, Exchange Public Folder, EMC Documentum, and Livelink. For different sources, refer to the different sections for details of how to use the tool.

Accessing DocAve Migrator Tool

To access the DocAve Migrator Tool complete the following steps:

1. Go to the installation directory of DocAve Agent, and browse to *…\AvePoint\DocAve6\Agent\bin*.
2. Double-click **MigratorTool.exe** to start this tool. The main interface appears.

***Note**: Make sure the user who runs DocAve Migrator Tool is a member of the local **Administrators** group on the server with DocAve Agent installed.

File System Migration

On the Migrator Tool main interface, click **File System Migration** to start. For a File System migration, use the Migrator Tool to complete the following steps:

- **Connection Management** – Edit, create, or delete a NetShare connection.
- **File Property Explorer** – Check the detailed information and permissions of files in the local device or a specific NetShare connection.
- **Scan Analysis** – Select the source file, configure scan analysis settings, and run a scan analysis job for evaluating the risks in your source content according to the scan analysis settings before executing the file system migration job.
- **Security Mappings –** Configure the domain mapping, group mapping, and user mapping and then export the security mappings information to the XML file.

Configuring Connection Management

Connection Management helps users to edit, create, or delete a NetShare connection. To create a new NetShare connection, complete the following steps:

1. Navigate to **Migrator Tool** > **File System Migration** > **Connection Management**.
2. Enter the **Connection Name**, **UNC Path**, and the corresponding **Username** and **Password**.

3. Click **Save** when you complete the settings.

To edit an existing NetShare connection, complete the following steps:

1. Select a NetShare connection in the **NetShare Connections** box.
2. Click **Edit** that appears at the end of the selected connection.
3. Modify the **Connection Name**, **UNC Path**, and the corresponding **Username** and **Password**.
4. Click **Save** when you complete the settings.

To delete an existing NetShare connection, complete the following steps:

1. Select a NetShare connection in the **NetShare Connections** box.
2. Click the delete (✕) button that appears at the end of the selected connection.
3. Click **OK** when the pop-up message displays to make sure that you really want to delete this connection.

Configuring File Property Explorer

To check the detailed information and permissions of files in the local device or a specific NetShare connection, complete the following steps:

1. Navigate to **Migrator Tool** > **File System Migration** > **File Property Explorer**.
2. Select **Local scope** if you want to check files in the local device. Select a specific **NetShare connection** if you want to check files in this connection.
3. Expand the data tree on the left pane to locate the desired folder. All of the files in this folder are displayed on the right pane. The **Name**, **Size**, **Date Modified**, and **Location** information is listed.
4. Select the desired file. The file's properties and permissions will be displayed in the **Permissions** and **Details** area.

Performing a Scan Analysis

Scan analysis evaluates the risks in your source content, according to the scan analysis settings before, executing a file system migration job. After a scan analysis job completes, you will get an Excel report for the risks defined by the threshold settings you have configured. To scan the specified source contents, complete the following steps:

1. Navigate to **Migrator Tool** > **File System Migration** > **Scan Analysis**.
2. Select the source content from the local device or a specific NetShare connection for scan.
3. Click **Next** after you select the desired source content, or click **New Scan** to clear the current selection and start a new scan.
4. Select a filter policy or create a new filter policy to filter your desired source objects for the scan. If you do not want to use a filter policy, skip this step.

5. Configure the **Scan Analysis Settings** to set the rules.

   ***Note**: The source content that matches the rules will be clarified and the details will be added to the comment in the scan report. For each scan option, you are required to define a classification for the content matching your settings. Select a classification category from the **Classification** drop-down list. In the generated scan report, the contents matching the scan options settings will be marked with the classification you specified in the **Classification** column to group the scan results.

   - **Blocked file types in SharePoint** – Click **Show Details** to view the file types that are blocked in SharePoint. You can delete or add file types in the text box according to your requirements.
   - **Character Length** –Configure Target SharePoint library/folder URL and character length limitation settings.
     - **Target SharePoint library/list URL** – Enter the destination SharePoint library/list URL into this text box in the format: **http://www.avepoint.net/sites/subsite/library/folder**.
     - **Length of the file name exceeds** – The default value is 80, and the scale you can set is from 1 to 128. If the character length of the file name (consisting of the file name, the period (.), and extension name) exceeds the limitation you set, the extra characters at end of the file name are pruned.
     - **Length of the folder name exceeds** – The default value is 60, and the scale you can set is from 1 to 128.
     - **Length of the SharePoint URL exceeds** – The default value is 255, and the scale you can set is from 1 to 260. The length of the SharePoint URL is calculated from the first character of the managed path, that is "/".
   - **File size exceeds** – Scan the item whose size exceeds the specified value. Enter the value in the blank text box and the unit is MB. By default, the item whose size exceeds 50 MB is scanned.
   - **Illegal characters in folder/file name in SharePoint** – Scan the files and folders whose name contains the illegal characters. Click **Show Details** to view the illegal characters. You can delete or add illegal characters in the text box according to your requirements.
   - **Folder name ended with illegal extensions** – Scan the folders with a name ending with an illegal extension name. For example, if is a folder named **abc_bylos** and **_bylos** is the illegal extension name, this folder will be clarified as the clarification category you set in the scan report. Click **Show Details** to view the illegal extension names.
   - **Folder/file name contains two consecutive periods (..)** – Scan the files and folders whose name contains consecutive periods.

6. Choose one of the following options:

   - Click **Next** to proceed to the next step.
   - Click **Back** to go to the previous step to review and modify your selection.

- Click **New Scan** to clear the current scan rules and go back to the **Source Data Selection** step.

7. Click **Browse** to select a location to store the scan report.
8. Click **Scan** to start the job. You can view the real-time progress.
9. After the scan is completed, **Scan Analysis Summary** information is listed, and you can find the scan report in the specified location to view detailed information.

Configuring Security Mappings

Configure Security Mappings to manage domain mappings, user mappings, and group mappings. Click the **Security Mappings** tab to access Security Mappings.

Configuring LDAP Settings

Before configuring the security mappings, you must configure **LDAP Settings** first by completing the following steps:

1. Click the **LDAP Settings** link. The **LDAP Settings** window appears.
2. In the **LDAP Settings** interface, configure the following settings:
    - **Type** – Choose to configure the settings for a source domain or a destination domain by selecting the corresponding radio button.
    - **LDAP Path** – Enter the IP address or host name of the server where the domain controller is installed.
    - **Username** – Enter the name of the user who has the permission to access the LDAP server.
    - **Password** – Enter the password of the user.
3. Click **Add** to save the LDAP settings. The domain information is displayed in the **Domains** table. Click **Reset** to clear the current configuration and configure new settings.
4. After configuring the LDAP settings for the source domain and the destination domain, click **Close** to close the **LDAP Settings** window.

Configuring Domain Mappings

To configure a domain mapping, click the **Domain Mapping** tab in the **Security Mappings** interface, and then complete the following steps:

1. Select a source domain in the **Source Domain Name** field.
2. Select a destination domain in the **Destination Domain Name** field.
3. Click **Add** to create a domain mapping. Click the delete ( ) button that appears at the end of the domain mapping to delete the mapping.
4. Click **Export to XML File** to export the mapping to an XML file.

***Note**: DocAve supports importing the exported domain mapping XML file to **Control Panel** > **Mapping Manager** > **Domain Mapping**.

***Note**: The configured domain mapping takes effect in a file system migration job once the following conditions are both met:

- The XML file is stored in *…\AvePoint\DocAve6\Agent\data\Migrator\FileMigrator* directory.
- The value of the attribute **ExternalSecurity** in **FileSystemMigrationConfiguration.xml** file is **True**. The **FileSystemMigrationConfiguration.xml** file resides in *…\AvePoint\DocAve6\Agent\data\Migrator\FileMigrator*.

Configuring User Mappings

To configure a user mapping, click the **User Mapping** tab in the **Security Mappings** interface, and then complete the following steps:

1. Select a source domain from the first drop-down list.
2. Click **Load** to access the **Load Source User** window.
3. Optionally, select the **Use filter rules** checkbox to filter the source users by configuring the following settings:
    a. Click **Add a Criterion** to add a filter rule.
    b. Select a rule from the **Rule** drop-down list to determine filter the source users by **Login Name**, **Display Name**, **First Name**, or **Last Name**.
    c. Select a filter condition from the **Condition** drop-down list to decide how to work on the filter rule. The selected rule **Starts With** or **Contains** the specified value. Select **By Regex** to filter users by regular expression.
    d. Enter your desired value or regular expression in the **Value** text box.

    Click **Add a Criterion** to and repeat the steps above to add multiple rules. There are two logics currently: **And** and **Or**. By default, the logic is set to **And**. If desired, change the logic to **Or** by selecting it from the drop-down list. **And** means the user that meets all of the filter criteria will be added to the user mapping. **Or** means the user that meets any one of the filter criteria will be added into the user mapping.

    Click the delete ( ) button to delete a filter rule.
4. Click **Load** to load the source users, and close the **Load Source User** window.
5. Select a source domain from the second drop-down list.
6. Click **Load** to access the **Load Destination User** window.
7. Optionally, select the **Use filter rules** checkbox to filer the source users. For details, refer to step 3.

8. Click **Load** to load the destination users and close the **Load Destination User** window.
9. The loaded source/destination users are displayed in the **Source Username**/**Destination Username** field.
10. Select a source user and a destination user, and then click **Add** to create a user mapping.
11. To add a new source or destination user, click **Add a Source User** or **Add a Destination User**. The **Add Users** window appears.
12. Click **Add** and enter the username in the text box, or click the delete ( ) button to delete the newly added user.
13. Click **Save** to save your configurations, or click **Cancel** to cancel your configurations.
14. On the right pane, select the **Show default matched users** checkbox to display the default matched users. The source users and the destination users are matched based on the login name without domain.

    For example, there is a source user **source\administrator** and a destination user **destination\administrator**. The name **administrator** is the same and they are matched.

    ***Note**: When the **Show default matched users** checkbox is selected, it is unsupported to manually add a user to the right pane.
15. Click **Export to XML File** to export the mapping to an XML file.

    ***Note**: DocAve supports importing the exported user mapping XML file to **Control Panel** > **Mapping Manager** > **User Mapping**.

    ***Note**: The configured user mapping takes effect in a file system migration job once the following conditions are both met:

    - The XML file is stored in *…\AvePoint\DocAve6\Agent\data\Migrator\FileMigrator* directory.
    - The value of the attribute **ExternalSecurity** in **FileSystemMigrationConfiguration.xml** file is **True**. The **FileSystemMigrationConfiguration.xml** file resides in *…\AvePoint\DocAve6\Agent\data\Migrator\FileMigrator*.

Configuring Group Mappings

To configure a group mapping, click the **Group Mapping** tab in the **Security Mappings** interface, and then complete the following steps:

1. Select a source domain from the first drop-down list.
2. Click **Load** to access the **Load Source Group** window.
3. Optionally, select the **Use filter rules** checkbox to filer the source groups.
    a. Click **Add a Criterion** to add a filter rule.

b. Select **Group Name** from the **Rule** drop-down list to filter the source groups by group name.

c. Select a filter condition from the **Condition** drop-down list to decide how to work on the filter rule. The group name **Starts With** or **Contains** the specified value. Select **By Regex** to filter groups by regular expression.

d. Enter your desired value or regular expression in the **Value** text box.

Click **Add a Criterion** to and repeat the steps above to add multiple rules. There are two logics currently. **And** and **Or**. By default, the logic is set to **And**. If desired, change the logic to **Or** by selecting it from the drop-down list. **And** means the group that meets all of the filter rules will be added to the group mapping. **Or** means the group that meets any one of the filter rules will be added into the group mapping.

Click the delete ( ) button to delete a filter rule.

4. Click **Load** to load the source groups and close the **Load Source Group** window.
5. Select a destination domain from the second drop-down list.
6. Click **Load** to access the **Load Destination Group** window.
7. Optionally, select the **Use filter rules** checkbox to filer the source users. For details, refer to step 3.
8. Click **Load** to load the destination groups and close the **Load Destination Group** window.
9. Click **Export to XML File** to export the mapping to an XML file.

   ***Note**: DocAve supports importing the exported group mapping XML file to **Control Panel** > **Mapping Manager** > **Group Mapping**.

   ***Note**: The configured group mapping takes effect in a file system migration job once the following conditions are both met:

   - The XML file is stored in *…\AvePoint\DocAve6\Agent\data\Migrator\FileMigrator* directory.
   - The value of the attribute **ExternalSecurity** in **FileSystemMigrationConfiguration.xml** file is **True**. The **FileSystemMigrationConfiguration.xml** file resides in *…\AvePoint\DocAve6\Agent\data\Migrator\FileMigrator*.

Exchange Public Folder Migration

Before performing an Exchange Public Folder Migration job, you can use the DocAve Migrator Tool to implement the following functions:

- Scan the source public folder contents. The contents in the selected nodes will be recorded in the scan report and the contents that match the configured rules will be marked with a comment for your reference.
- Configure the security mapping. DocAve Migrator tool can export the security mapping settings to an XML file and you can import this XML file to DocAve for use in running migration jobs.

To access the Exchange Public Folder Migration section of DocAve Migrator tool, click **Exchange Public Folder Migration** on the **DocAve Migrator Tool** main interface. The **Exchange Public Folder Migration** interface appears with the **Connection Management** page selected.

***Note**: Make sure the tool you launched is at the machine that can connect to the Exchange Server.

Refer to the following sections below for details about configuring the Exchange Public Folder connection settings, performing the scan analysis, and configuring security mapping settings.

Configuring Exchange Public Folder Connection

To perform the scan, you must configure the Exchange public folder connection so that the tool can access the Exchange Public Folder by completing the following steps:

1. In the **Connection Management** interface, find the **Configure Exchange Connection** area.
2. Configure the following settings:
    - **Connection Name** – Enter a name in the text box for the Exchange public folder connection.
    - **Access Method** – Select the access method according to the Exchange server.
        - Select **WebDAV (Exchange 2000/2003/2007)** if using Exchange Server 2000/2003/2007.
        - Select **Web Services (Exchange 2007/2010/2013)** if using Exchange Server 2007/2010/2013.
        - Select **MAPI (Exchange 2000 or above versions)** if using Exchange Server 2000 or above versions.

          ***Note**: The 32-bit Microsoft Outlook whose version is Microsoft Outlook 2003 Service Pack 2 or above must be installed on the source Agent, if you select the **MAPI** access method.

        For Exchange Server 2007, both **WebDAV** and **Web Services** are applicable.

    - **Username** and **Password –** Enter the username (domain\username) and the password for accessing Exchange Public Folder. It is recommended to specify an administrator here in order to have the required permission to load all data.
    - **Exchange URL** (for WebDAV and Web Services) – Enter the URL of the Exchange Public Folder that the tool accesses to. An example is shown in the **Exchange URL** text box.

- **Outlook Profile** (for MAPI only) – Enter the Outlook profile that the tool accesses to.

  ***Note**: You can find the existing profiles by navigating to **Control Panel** > **Mail (32-bit)** > **Show Profiles** on the source server. If no profile can be found, create a new one.

3. Click **Save** to save this connection, or click **Reset** to reset the connection. The saved connection will be listed in the **Exchange Connections** area below.
4. In the **Exchange Connections** area, click **Edit** in each line to edit the corresponding connection, or click the delete (✕) button to delete the connection.

Scanning

After configuring the Exchange connections, click **Scan Analysis** to go to the **Scan Analysis** interface. There are three steps to perform the scan analysis: **Source Data Selection**, **Scan Analysis Settings**, and **Scan and Results**.

Source Data Selection

In the **Source Data Selection** step, configure the settings by completing the following steps:

1. Select an existing Exchange connection from the drop-down menu, or click **New Exchange Connection** to create a new Exchange connection directly in the **Configure Exchange Connection** pop-up window. For detailed information on create a new connection, refer to Configuring Exchange Public Folder Connection.
2. Click the **Public Folders** to expand the data tree, and select the nodes that you want to scan.
3. Click **Next** to go to step 2, or click **New Scan** to restart the step 1's configuration.

Scan Analysis Settings

In the **Scan Analysis Settings** step, configure the scan analysis settings to set the rules. The source contents matching the rules will be marked with a comment in the scan report. For each scan option, select a classification from the **Classification** drop-down menu. In the scan report, the contents matching the scan options will be marked with the classification you specified in a **Classification** column to help you group the scan results.

For detailed information on the scan options, refer to the following steps:

1. **Filter Policy** – Select an existing filter policy from the drop-down menu, or click **New Filter Policy** to create a new one. You can also click **Filter Policy Settings** to create new filter policies or manage the existing ones. For detailed information, refer to Filter Policy Management.
2. **Block file types in SharePoint** – Click **Show Details** to view the file types that are blocked in SharePoint. You can delete or add file types in the text box according to your requirements.
3. **Character Length** – Configure character length limitations for the SharePoint URL, filename, and folder name. In SharePoint, the maximum length of SharePoint URL is **260** characters, and the maximum length of file name and folder name is **128** characters.

- **Length of the file name exceeds** – The default value is 60, and the scale you can set is from 1 to 128. If the character length of the file name (consisting of the file name, the period (.), and extension name) exceeds the limitation you set, the extra characters at end of the file name are pruned.
- **Length of the folder name exceeds** – The default value is 80, and the scale you can set is from 1 to 128.
- **Length of the SharePoint URL exceeds** – The default value is 255, and the scale you can set is from 1 to 260. The length of the SharePoint URL is calculated from the first character of the managed path, that is "/".

To check whether the length of the SharePoint URL exceeds the limitation, you must specify the length of your destination SharePoint URL by one of the following methods:

- **Target SharePoint URL** – Enter the URL of the destination SharePoint site.
- **Target SharePoint URL length** – Enter the length of the destination SharePoint site URL. The length of the SharePoint site URL is calculated from the first character of the managed path, that is "/".

4. **Illegal characters in folder/file name in SharePoint** – Scan the files and folders whose name contains the illegal characters. Click **Show Details** to view the illegal characters. You can delete or add illegal characters in the text box according to your requirements.
5. **File size exceeds** – Scan the file whose size exceeds the specified value. Enter the value in the blank text box and the unit is MB. The default value is **50MB**.
6. **Attachment Information** – Scan the attachment information in each item.

   ***Note**: Scanning the attachment information may take a long time.

   - **Attachment size exceeds** – Scan the attachments whose size is larger than the specified value. Enter a value in the corresponding text box and the unit is **KB**.
   - **Attachment numbers exceeds** – Scan the number of attachments in an item that is more than the specified value. Enter a value in the corresponding text box.
7. **Hidden items** – Scan all of the hidden items in this source.
8. **Folder/file name ends with illegal postfixes** – Scan the files and folders with a name ending with an illegal postfix. For example, if is a folder named **abc_bylos** and **_bylos** is the illegal postfix, this folder will be included in the scan report. Click **Show Details** to view the illegal postfixes.
9. **Folder/file name contains two consecutive periods (..)** – Scan the files and folders whose name contains consecutive periods.
10. **Users and Groups** – Scan the users and groups that have permissions to the selected nodes.

Click **Next** to go to step 3, or click **New Scan** to restart the step 1's configuration.

Scan and Results

In the **Scan and Results** step, click **Browse** to browse to a location to store the scan report, and click **OK** to save the location, and then click **Scan** to start the scan process. You can view the following information under the lower pane of the **Scan Analysis** interface: **Scan Progress** and **Scan Analysis Summary** (including **Number of Scanned Folders**, **Number of Scanned Items**, **Number of Scanned Attachments**, **Total Size**, and **Start Time**). When the scan progress is finished, you can view the **Finish Time** of the scanning. You can also click **View Detailed Report** to locate to the specified location to view the report directly.

Filter Policy Management

To create new filter policies or manage the existing ones, click **Filter Policy Settings** in the **Scan Analysis Settings** interface. The **Filter Policy** pop-up window appears. Configure the following settings:

- **Create** – To create a new filter policy, click **Create**. The **Create** interface appears.
    i. Enter a name for the filter policy you are about to create.
    ii. Select a filter level (**Folder** or **Exchange Message**) and click **Add a Criterion**.
    iii. In the **Rule** column, **Name** is the default rule for an Exchange message and a folder. **Contains** is the default condition.
    iv. Click **Name** to change the rule from the drop-down menu and then specify the corresponding condition and value.

    For the **Name** and **Message Class** rule, the available conditions are **Contains**, **Does Not Contain**, **Equals**, and **Does Not Equal**.

    ***Note**: Only the **Name** rule is available if you select the **Folder** level.

    - **Contains** – When the item's name/message class contains the value you set, it will be filtered and included in the filter results.
    - **Does Not Contain** – When the item's name/message class does not contain the value you set, it will be filtered and included in the filter results.
    - **Equals –** When the item's name/message class equals the value you set, it will be filtered and included in the filter results.
    - **Does Not Equal –** When the item's name/message class does not equal the value you set, it will be filtered and included in the filter results.

    For the **Created Time**/**Modified Time**/**Received Time**/**Start Time**/**Due Time** rule, the available conditions are **Before**, **After**, **Within**, and **Older Than**.

    ***Note**: Only the **Created Time** and **Modified Time** rules are available if you select the **Folder** level.

- **Before** – When the item's time is before the time value you set, it will be filtered and included in the filter results.
- **After** – When the item's time is after the time value you set, it will be filtered and included in the filter results.
- **Within** – When the item's time is within the time range you set, it will be filtered and included in the filter results.
- **Older Than** – When the item's time is older than the time value you set, it will be filtered and included in the filter results.

v. If you have more than one criterion, click the order to adjust the criteria's order and adjust the logic relation according to your requirements. By default, the logic relation between each criterion is **And**. You can click the current logic relation (**And** or **Or**) to change it.

- **And** – When multiple criteria are used, only the data that meets all of the criteria is included in the filter results.
- **Or** – When multiple criteria are used, the data that matches at least one of the criteria is included in the filter results.

vi. After the filter policy settings complete, click **Save** to save the settings and return to the **Filter Policy** page.

- **Edit** – Select an existing filter policy and click **Edit**. The **Edit** interface appears. Configure the filter rules and click **Save** to save changes to this filter policy.
- **Delete** – Select an existing filter policy and click **Delete**.

Configuring Security Mapping

To configure the domain mapping, group mapping, and user mapping, complete the following steps. DocAve Migrator tool can generate the mapping settings to an XML file for using by DocAve.

1. Click **Security Mappings** to go to the **Configure Security Mappings** interface.
2. Click the **LDAP Settings** link to configure the LDAP (Lightweight Directory Access Protocol) settings. The **LDAP Settings** pop-up window appears.
3. In the **LDAP Settings** area, select the **Source Domain Name**/**Destination Domain Name** option and provide the following information.
    - **Exchange Version** (for Source Domain only) – Enter the version of the Exchange server.
    - **LDAP Path** – Enter the IP address where the domain controller is installed.
    - **Username** and **Password** – Specify the credentials.
4. Click **Add** to save the domain, or click **Reset** to reset the settings. After successfully verifying the settings, the domain will be displayed in the **Domains** area.

5. If you want to migrate the source users and groups, click **Save Security Information** to save the Exchange user and group information to the **ExchangeSecurityInfo.xml** file. During the migration job, DocAve will use this file to obtain the exact security information instead of using API.

   ***Note**: To make this file take effect, save this file to the …*DocAve6**Agent**data**Migrator**PublicFolderMigrator* directory.

6. Click **Close** or the close ( ) button on the upper-right corner of the pop-up window to close this window and back to the **Configure Security Mappings** interface.
7. Configure the mappings:
   a. **Domain Mapping** – Select a source domain from the **Source Domain Name** list and a destination domain from the **Destination Domain Name** list, then click **Add** to add the domain mapping. The mapping will be displayed on the right pane of the interface. You can click the **Delete** ( ) button to delete the selected domain mapping.
   b. **User Mapping** – Select a source/destination domain from the drop-down menu and click **Load**. The **Load Source/Destination User** pop-up appears. If desired, configure user filter rules by selecting the **Use filter rules** checkbox and add criteria to filter users. Click **Load** to load the users that meet the rules and back to the **Configure Security Mapping** interface. Select a source user from the **Source Username** list and a destination user from the **Destination Username** list, and then click then click **Add** to add the user mapping to the right pane of the interface. Click **Add a Destination User** to launch the **Add Users** pop-up window. Click **Add** to add a new user to be created in the destination and click **Save** to save the changes. Select the **Show default matched users** checkbox to show the default matched users. You can click the **Delete** ( ) button to delete the selected user mapping.
   c. **Group Mapping** – Select a source/destination domain from the drop-down menu and click **Load**. The **Load Source/Destination Group** pop-up appears. If desired, configure group filter rules by selecting the **Use filter rules** checkbox and add criteria to filter groups. Click **Load** to load the groups that meet the rules and back to the **Configure Security Mapping** interface. Select a source group from the **Source Group Name** list and a destination group from the **Destination Group Name** list, and then click the **Add** button to add the group mapping to the right pane of the interface. Click **Add a Destination Group** to launch the **Add Groups** pop-up window. Click **Add** to add a new group to be created in the destination and click **Save** to save the changes. Select the **Show default matched users** checkbox to show the default matched groups. You can click the **Delete** ( ) button to delete the selected group mapping.
8. After configuring the mappings, click **Export to XML File** to save the mapping settings to XML files. Each mapping type has its own XML file. You can import this XML file to DocAve when configuring the security mapping settings.

Lotus Notes Migration

On the Migrator Tool main interface, click **Lotus Notes Migration** to start. In the Lotus Notes Migration interface, you can analyze/scan the source objects and configure user mapping/content type mapping/InfoPath mapping.

Configuring Database Connections

Before analyzing/scanning the source objects or configuring user mapping/content type mapping/InfoPath mapping, you need configured database connections to select available databases.

To create the database connection, complete the following steps:

1. In the homepage of Lotus Notes Migration, click **File** on the ribbon.
2. Select **New Database Connection**, or click the new database connection (+) button. The **New Database Connection** window appears.
3. Configure the following settings:
    a. **INI File** – The INI file can be found in the path where the valid users of Lotus Notes are saved. By default, the path is *…\lotus\notes\notes.ini*. Click **Browse…** to set a new path.
    b. **User ID** – Select a User ID file from the drop-down list. When the INI file is selected by clicking **Browse…**, click **Load** to load the User ID files.
    c. **Password** – Enter the password of the user that you have selected in User ID file.
    d. **Domino Server** – Click **Load** to load the Domino Servers, and select your desired Domino Servers from the drop-down list.
    e. **Browse NSF files from local device** – Select the checkbox and click **Browse…** to browse the specific NSF files from your local device.
4. Click **Test Connection** to verity the connection configurations.
5. Click **Save** to save the database connection.

    Optionally, select the **Create another** checkbox. After clicking **Save**, the currently configured database connection will be saved and the **New Database Connection** interface will be cleared for creating a new database connection.

    In the homepage of Lotus Notes Migration, the previously created database connections are displayed on the left pane.

6. Double-click a database connection and the Domino Server's databases are displayed on the right pane. The following information of each database is displayed: the title, the database file name, the category, the template, the number of the documents in it, the total size, the server where it is, the created time, and the last modified time.

To edit a database connection, right-click the database connection and click **Edit**. The **Edit Database Connection** window appears. Refer to the steps above the edit the information.

To delete a database connection, right-click the database connection and click **Delete**.

To refresh a database connection, right-click the database connection and click **Refresh**.

Exporting DXL File

DocAve Migrator Tool allows you to export DXL file for Lotus Notes data.

To export DXL files, complete the following steps:

1. In the homepage of Lotus Notes Migration, select one or more databases on the right pane.
2. Click **File** on the ribbon.
3. Click **Export DXL File**. The **Export DXL File** window appears.
4. Select a database from the **File Name** drop-down list, and then select one of the following options:
    - **Export all documents** – Exports DXL file for all Lotus Notes documents.
    - **Export specific documents filtered by Lotus Notes formula** – Export DXL file for specific Lotus Notes documents. Enter a Lotus Notes formula in the text box to filter the documents.
5. Click **Export** to export DXL file immediately.

Configuring Content Type Mappings

Configure content type mappings to map the Lotus Notes form to the specified SharePoint content type.

Creating a Content Type Mapping for a Single Database

To create a new content type mapping for a single database, complete the following steps:

1. In the homepage of Lotus Notes Migration, select a database on the right pane.
2. Choose one of the following methods to access the **New Content Type Mapping** window:
    - Click **Mapping** on the ribbon, and then click **Content Type Mapping** to select **New Mapping**.
    - Click the new content type mapping ( ) button.
    - Right-click the database and click **New Content Type Mapping**.
3. In the left **Lotus Notes Forms** list, all forms are selected by default, which means each form will be mapped to corresponding SharePoint content type. To map the specified forms to the destination, only select the checkbox before the form name.

4. Double-click a form and the default mapping settings are displayed. Review the following information:

    - On the top pane, view the following information.
        - **SharePoint Content Type Name** – The name of the SharePoint content type that the form maps to. You can change the name by entering the customized name.
        - **Specified Title** – Use the value of a specified field as the title of an item in SharePoint. You can select a field from the drop-down list.
        - **Migrate Response To** – Choose whether to add the **Response To** column in the destination. By default, the checkbox is selected.
    - On the right pane, all fields contained in the selected form and the column mapping for each field are displayed.
        - For each column mapping, the following information is displayed: the field name, the field type, the name of the SharePoint column that the field maps to, the SharePoint column type, and the order of the column. You can double-click the field name, field type, or column name to edit it, select another column type from the drop-down list, and adjust the order by selecting the new order from the drop-down list.
        - For each column mapping, configure whether to use the column mapping by selecting/deselecting the **Included** checkbox, configure whether to hide the column in the destination by selecting/deselecting the **Hidden** checkbox, and configure whether to show the column in the default view by selecting/deselecting the **Show In Default View** checkbox.
5. If you want to add a new column mapping, click **Add Row** to set up a new column mapping. Enter the field title, the filed type, the column name, select the column type and the order, and configure the **Hidden**, **Included**, **Show In Default View** settings. If you want to delete a column mapping, select the mapping and click **Delete Row** to delete a column mapping.
6. Click **Generate** to generate the mapping file **LotusNotesContentType.Domino web access.xml** (**Domino web access** is the database name). By default, this file is saved in the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\ContentTypeMapping* directory.

    ***Note**: Only when the file is in this directory, it will take effect in a Lotus Notes Migration job.

Editing an Existing Content Type Mapping

To modify an existing content type mapping, complete the following steps:

1. In the homepage of Lotus Notes Migration, click **Mapping** on the ribbon.
2. Click **Content Mapping** to select **Edit an Existing Mapping**, or click the edit an existing mapping ( ) button.
3. Select your desired content type mapping XML file in the pop-up window. The **Configure Content Type Mapping** interface appears. For details, refer to Creating a Content Type Mapping for a Single Database.

Creating Content Type Mappings for Multiple Databases

To create content type mappings for multiple databases, complete the following steps:

1. In the homepage of Lotus Notes Migration, select multiple databases on the right pane.
2. Choose one of the following methods to access the **Configure Content Type Mapping** window.
    - Click **Mapping** on the ribbon, and then click **Content Type Mapping** to select **Create Mapping for Multiple Databases**.
    - Click the new content type mapping ( ) button
3. Select a database from the **File Name** drop-down list.
4. In the left **Lotus Notes Forms** list, all forms are selected by default, which means each form will be mapped to corresponding SharePoint content type. To map the specified forms to the destination, only select the checkbox before the form name.
5. Double-click a form and the default mapping settings are displayed. Review the following information:
    - On the top pane, review the following information:
        - **SharePoint Content Type** – The name of the SharePoint content type that the form maps to. You can change the name by entering the customized name.
        - **Specified Title** – Use the value of a specified field as the title of an item in SharePoint. You can select a field from the drop-down list.
        - **Migrate Response To** – Choose whether to add the **Response To** column in the destination.
    - On the right pane, all fields contained in the selected form and the column mapping for each field are displayed.
        - For each column mapping, the following information is displayed: the field name, the field type, the name of the SharePoint column that the field maps to, the SharePoint column type, and the order of the column. You can double-click the field name, field type, or column name to edit it, select another column type from the drop-down list, and adjust the order by selecting the new order from the drop-down list.
        - For each column mapping, configure whether to use the column mapping by selecting/deselecting the **Included** checkbox, configure whether to hide the column in the destination by selecting/deselecting the **Hidden** checkbox, and configure whether to show the column in the default view by selecting/deselecting the **Show In Default View** checkbox.
6. If you want to add a new column mapping, click **Add Row** to set up a new column mapping. Enter the field title, the filed type, the column name, select the column type and the order, and configure the **Hidden**, **Included**, **Show In Default View** settings. If you want to delete a column mapping, select the mapping and click **Delete Row** to delete a column mapping.

7. Click **Generate All** to generate the mapping files. By default, the files are saved in the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\ContentTypeMapping* directory.

   ***Note:** The files will only take effect in the Lotus Notes Migration jobs when they are saved in this directory.

Configuring User Mappings

Lotus Notes Migration supports the following types of user mappings:

- User Mapping for ACL Users in Database
- User Mapping for Address Book Database
- User Mapping for FBA Users

User Mapping for ACL Users in Database

To configure a user mapping for ACL users in databases, complete the following steps:

1. In the homepage of Lotus Notes Migration, select one or more databases on the right-pane.
2. Choose one of the following methods to access the **Configure User Mapping** window.
   - Click **Mapping** on the ribbon, and then click **User Mapping** to select **New User Mapping for ACL Users in Database**.
   - Right-click a database and click **New User Mapping for ACL Users in Database**.
3. Click the **Local Configuration** link to retrieve user information.
4. In the **Local Configuration** window, enter the Domino Server name and the address book database name. Click **Save** to save the local configuration and close the **Local Configuration** window.
5. Click the **LDAP Settings** link in **Please configure LDAP Settings to manage domains**.
6. In the **LDAP Settings** window, enter the following information:
   - **Path** – Enter the IP address or host name where the domain controller is installed.
   - **Username** – Enter the name of the user that has the permission to access the LDAP server.
   - **Password** – Enter the user's password.
7. Click **Save** to save the current LDAP settings, or click **Reset** to clear the entered information and configure the settings again.

   The saved LDAP path is added into the **Domain** section. You can edit the LDAP setting by selecting the LDAP path and clicking **Edit**. Edit the information in the **Browse a Domain** section. To delete an LDAP setting, select the LDAP path, and then click the delete (✕) button.

8. Click **Close** to close the **LDAP Settings** window and go back to the **Configure User Mapping** window.
9. Select a previously configured LDAP path from the **User Mapping** drop-down list. The domain users are loaded in the **Domain Users** section. The Lotus Notes users are displayed in the right pane.
10. Select a Lotus Notes user, and then double-click the domain user to create the mapping. The domain user appears in the **SharePoint User** column, and display name of the selected SharePoint user is updated in the **Display Name** column. You can also enter your desired SharePoint username and display name in the corresponding text boxes.
    - For each mapping you created, you can select whether to use it by selecting/deselecting the **Included** checkbox.
    - Click **Add Row** to add a new user mapping. Enter the Lotus Notes username and then double-click a domain user to create the mapping.
    - If you want to delete a user mapping, select the mapping and click **Delete Row** to delete a user mapping.
11. After configuring the user mapping, choose one of the following options:
    - **Save** – Click **Save** to save the configurations into one XML file. The mapping file will be saved in the default **LotusNotesUserInfo.default.xml** file, which is located in the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\UserMapping* directory.
    - **Save into Multiple XML Files** – Click this button to save the user mapping files into multiple XML files (which is convenient for editing). The **Partition Options** window appears.
      - **Files** – The number of XML files that you want to get.
      - **Records** – The number of user mapping records in one XML file.

      Click **OK** to save the XML files.
    - **Cancel** – Click **Cancel** to cancel your user mapping configuration.

User Mapping for Address Book Database

To configure the user mapping for Address Book database, complete the following steps:

1. In the homepage of Lotus Notes Migration, select an Address Book database on the right pane.
2. Choose one of the following methods to access the **Configure User Mapping** window.
    - Click **Mapping** on the ribbon, and then click **User Mapping** to select **New User Mapping for Address Book Database**.
    - Click the new user mapping for address book database ( ) button.
    - Right-click an Address Book database and click **New User Mapping for Address Book Database**.

3. Click the **LDAP Settings** link in **Please configure LDAP Settings to manage domains**.
4. On the **LDAP Settings** window, enter the following information:
    - **Path** – Enter the IP address or host name where the domain controller is installed.
    - **Username** – Enter the name of the user that has the permission to access the LDAP server.
    - **Password** – Enter the user's password.
5. Click **Save** to save the current LDAP settings, or click **Reset** to clear the entered information and configure the settings again.

    The saved LDAP path is added into the **Domain** section. You can edit the LDAP setting by selecting the LDAP path and clicking **Edit**. Edit the information in the **Browse a Domain** section. To delete an LDAP setting, select the LDAP path, and then click the delete ( ) button.
6. Click **Close** to close the **LDAP Settings** window and go back to the **Configure User Mapping** window.
7. Select a previously configured LDAP path from the **User Mapping** drop-down list. The domain users are loaded in the **Domain Users** section. The Lotus Notes users are displayed in the right pane.
8. You can set up the mapping manually or automatically:
    - **Manually** – Select a Lotus Notes user, and then double-click the domain user to create the mapping. The domain user appears in the **SharePoint User** column, and display name of the selected SharePoint user is updated in the **Display Name** column.
        - For each mapping you created, you can select whether to use it by selecting/deselecting the **Included** checkbox.
        - Click **Add Row** to add a new user mapping. Enter the Lotus Notes username and then double-click a domain user to create the mapping.
        - If you want to delete a user mapping, select the mapping and click **Delete Row** to delete a user mapping.
    - **Automatically** – Click **User Mapping Condition** to set the conditions for matching the domain user and the Lotus Notes user automatically. You can configure **User Mapping Condition** and/or **User Filter Policy**.
        - **User Mapping Condition** – Configure the condition to automatically match the domain user with Lotus Notes user.
            - **Match Mode** – Select the match mode for the conditions. If selecting **Combine**, the user mapping will be automatically created when all selected conditions are matched. If selecting **Union**, the user mapping will be automatically created for the users that match one of the conditions. By default, **Union** is selected.
            - **Match by first name** – Automatically creates the user mapping for the domain user and the Lotus Notes user who have the same first name.

        - **Matched by last name** – Automatically creates the user mapping for the domain user and the Lotus Notes user who have the same last name.
        - **Matched by e-mail address** – Automatically creates the user mapping for the domain user and the Lotus Notes user who have the same e-mail address.
    - **User Filter Policy** – Configure user filter policy to filter Lotus Notes users that will be added into the user mapping. Click **Add a Criterion**. A new row appears.
        - Select a filter rule from the **Rule** drop-down list to filter by **First Name**, **Last Name**, or **E-mail Address**.
        - Select a filter condition from the **Condition** drop-down list to decide how to work on the filter rule. The selected rule **Starts With** or **Contains** the specified value. Select **By Regex** to filter users by regular expression.
        - Enter your desired value or regular expression in the **Value** text box.

      Click **Add a Criterion** to and repeat the steps above to add multiple criteria. There are two logics currently. **And** and **Or**. By default, the logic is set to **And**. If desired, change the logic to **Or** by selecting it from the drop-down list. **And** means the user that meets all of the filter criteria will be added to the user mapping. **Or** means the user that meets any one of the filter criteria will be added into the user mapping.

      Click the delete ( ) button to delete a filter criterion.

  Click **Load** to add the users to the user mapping and close the **User Mapping Condition** window.

9. After configuring the user mapping, choose one of the following options:

    - **Save** – Click **Save** to save the configurations into one XML file. The mapping file will be saved in the default **LotusNotesUserInfo.default.xml** file, which is located in the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\UserMapping* directory.
    - **Save into Multiple XML Files** – Click this button to save the user mapping files into multiple XML files (which is convenient for editing). The **Partition Options** window appears.
        - **Files** – The number of XML files that you want to get.
        - **Records** – The number of user mapping records in one XML file.

      Click **OK** to save the XML files.
    - **Cancel** – Click **Cancel** to cancel your user mapping configuration.

User Mapping for FBA Users

To configure the FBA user mapping, complete the following steps:

1. In the homepage of Lotus Notes Migration, select an Address Book database on the right pane.
2. Choose one of the following methods to access the **Configure FBA User Mapping** window.
    - Click **Mapping** on the ribbon, and then click **User Mapping** to select **New FBA User Mapping**.
    - Click the new FBA user mapping ( ) button.
    - Right-click an Address Book database and click **New FBA User Mapping**.
3. Click the **FBA Settings** link in **Please configure FBA Settings to manage membership providers**.
4. On the **FBA Settings** window, enter the following information:
    - **Membership Provider Name** – Enter the name of the membership provider.
    - **Server** – The IP address or the host name of the SQL server.
    - **Protocols** – Select a protocol from the drop-down list, you can select **TCP/IP** or **Named Pipes**. If you select TCP/IP, select the port number of the SQL server.
    - **Database** – Enter the FBA database name.
    - **Username** and **Password** – Specify the credentials to the FBA database. Enter the username and password in the corresponding text boxes.
5. Click **Save** to save the settings, or click **Reset** to clear the entered information and configure the settings again.

    The saved membership provider is added into the **Domain** section. You can edit the membership provider by selecting it and clicking **Edit**. Then, edit the information in the **Browse a Membership Provider** section. To delete a piece of membership provider, select it, and then click the delete ( ) button.
6. Click **Close** to close the **FBA Settings** window and go back to the **New FBA User Mapping** window.
7. Select a previously configured membership provider from the **FBA User Mapping** drop-down list. The FBA users are loaded in the **FBA User** section. The Lotus Notes users are displayed on the right pane.
8. Select a Lotus Notes user and then double-click the FBA user to create the mapping. The FBA user appears in the **FBA User** column and the display name of the selected FBA user is updated in the **Display Name** column. For each mapping you created, you can select whether to use it by selecting/deselecting the **Included** checkbox.
9. Click **Generate** to generate the FBA mapping XML file into the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\UserMapping* directory.

Editing an Existing User Mapping

To modify an existing user mapping, complete the following steps:

1. In the homepage of Lotus Notes Migration, click **Mapping** on the ribbon.

2. Click **User Mapping** to select **Edit an Existing Mapping**, or click the edit an existing mapping ( ) button.
3. Select your desired user mapping XML file in the pop-up window. The **Configure User Mapping** interface appears. For details, refer to User Mapping for ACL Users in Database, User Mapping for Address Book Database, or User Mapping for FBA Users.

Configuring InfoPath Mappings

To configure the InfoPath mapping, complete the following steps:

1. In the homepage of Lotus Notes Migration, select a database on the right pane.
2. Choose one of the following methods to access the **InfoPath Mapping** window.
    - Click **Mapping** on the ribbon, and then click **Generate InfoPath Mapping and Publish InfoPath Template**.
    - Right-click a database and click **InfoPath Mapping**.
3. In the **Generate InfoPath Template** step, double-click a Lotus Notes form and the columns contained in it are displayed on the right pane, including the information of the column name and the column type. For each column, configure the InfoPath mapping as follows:
    a. Double-click the InfoPath column name to edit it.
    b. Select the **InfoPath** column type from the drop-down list.
    c. If you want to add the column into the InfoPath template, select the **Add to Template** checkbox. Otherwise, deselect this checkbox.
4. Click **Generate Template** to generate the InfoPath template file in the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\InfoPathTemplate* directory. In this directory, a folder named by the database and an InfoPath template file are generated. The file name is the same as the Lotus Notes form you selected.
5. Click **Next** to go to the **Publish** step.
6. In the **SharePoint Connection** section, configure the following settings:
    - **SharePoint Site URL** – Enter the URL of the SharePoint site where you want to publish the InfoPath file.
    - **Library Name** – Enter the name of the library where you want to publish the InfoPath file.
    - **Username** – Enter the username. The user must have the Full Control permission to the site.
    - **Password** – Enter the password of the user.
7. Click **Test** to check whether the site exists and whether the user has enough permission.
8. Click **Publish** to publish the InfoPath file to SharePoint, and use DocAve to run the migration job to convert the source documents to InfoPath format.

9. Click **Next** to go to the **Generate InfoPath Mapping** step, or click **Back** to go back to the previous step to review and modify your configurations.
10. Double-click a Lotus Notes form on the left pane and the columns contained in it are displayed on the right pane, including the information of the column name and the column type. For each column, configure the InfoPath mapping as follows:
    a. Double-click the InfoPath column name to edit it.
    b. Select the InfoPath column type from the drop-down list.
    c. If you want to add the column into the InfoPath mapping, select the **Add to Mapping** checkbox. Otherwise, deselect this checkbox.
    d. If you want to add a new column, click **Add Row**. If you want to delete a column, select the column and click **Delete Row**.
11. Click **Generate InfoPath Mapping** to generate the InfoPath mapping file in the *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\InfoPathMapping* directory.
12. Click **Cancel** to finish the configurations and close the **InfoPath Mapping** window.
13. In DocAve Manager, navigate to **Lotus Notes Migration** > **Profile Settings** > **Migration Options**> **Document Format Option**. Select the **Convert Lotus Notes documents to** checkbox and select **InfoPath** from the drop-down list. Apply this profile to run a migration job and the source documents will be converted to the InfoPath format.

Performing a Scan Analysis

Before performing a migration job, you can scan the source databases, views, documents, and files. According to your configurations, you can determine the risk that will occur in the migration job.

1. In the homepage of **Lotus Notes Migration**, double-click a Database Connection to expand it.
2. Select your desired databases on the right pane.
3. Choose one of the following methods to access the **Scan Analysis** window.
    - Click **Analyzer** and select **Scan Analysis** on the ribbon.
    - Click the scan analysis () button.
    - Right-click a database and click **Scan Analysis**.
4. Optionally, select a previously configured filter policy from the drop-down list to filter your desired source objects for the scan, or click **New Filter Policy** to create a new one. Click **Filter Policy Settings** to manage all of the filter policies. For more information, refer to Managing Filter Policies.
5. Configure the options in **Scan Analysis Settings** to define the scan criteria. For each piece of information, you can classify its severity as **Information**, **Warning**, or **Critical**.
    - **Database Risk Information** – Scan the Lotus Notes databases to check whether there are risks for migration.

- **Form name contains illegal characters** – Check whether there are forms whose names contain illegal characters. Click **Show Details** and the default illegal characters are displayed. You can add new illegal characters or delete the existing illegal characters.
- **The number of fields exceeds the limitation of columns in SharePoint** – Check whether the number of the source fields exceeds the limitation of the destination columns in SharePoint.

- **View Risk Information** – Scan the Lotus Notes views to check whether there are risks for migration.
  - **Unsupported custom view** – Check whether there are custom views that are unsupported to be migrated to SharePoint.
- **Document Risk Information** – Scan the Lotus Notes documents to check whether there are risks for migration.
  - **Unsupported document elements for Lotus Notes Migration** – Check whether there are document elements that are unsupported to be migrated to SharePoint.
  - **Unsupported OLE object types for Lotus Notes Migration**– Check whether there are OLE object types that are unsupported to be migrated to SharePoint.
- **File Risk Information** – Scan the source files to check whether there are risks for migration.
  - **Blocked file types in SharePoint** – Check whether there are files types that will be blocked when being migrated to SharePoint. Click **Show Details** and the default blocked file types are displayed. You can add new file types and delete the existing file types.
  - **Length of the file name exceeds** – Check whether there are files with filename lengths exceeding the specified value. By default, the value is **80**. You can define your desired value from 1 to 128.
  - **Length of the SharePoint URL exceeds** – Enter SharePoint library/folder URL in the provided text box and check whether the URLs exceeds the specified value. By default, the value is **255**. You can define your desired value from 1 to 260.
  - **File size exceeds** – Check whether there are files with a size exceeding the specified size. By default, the size is **50 MB**. You can enter your desired value in the text box.
  - **File name contains illegal characters** – Check whether there are files with filenames containing illegal characters. Click **Show Details** and the default illegal characters are displayed. You can add new illegal characters and delete the existing illegal characters.
  - **File name contains two consecutive periods (..)** – Check whether there are files with filenames containing two consecutive periods.

6. Click **Next** to go to the **Scan and Results** step. Click **Browse…** to select a location to store the scan report, and then click **Scan** to start scanning.
7. After the scan is completed, the **Scan Analysis Summary** is listed. Go to the specified location to find the scan analysis report and view detailed information.

Managing Filter Policies

To manage filter policies, click **Filter Policy Settings** in the **Scan Analysis Settings** interface. You can create, edit, and delete a filter policy.

- **Create** – Click **Create** on the ribbon to create a new filter policy. For more information, refer to Configuring a Filter Policy.
- **Edit** – Select a filter policy and click **Edit** on the ribbon to change the configurations for the selected filter policy. For more information, refer to Configuring a Filter Policy.
- **Delete** – Select one or more filter policies and click **Delete** on the ribbon. A confirmation window appears, confirming that you want to proceed with the deletion. Click **OK** to delete the selected filter policies, or click **Cancel** to return to the **Filter Policy** interface without deleting the selected filter policies.

Configuring a Filter Policy

To create a new filter policy, click **New Filter Policy** from the drop-down list and complete the steps below:

1. **Filter Policy Name** – Enter a name for this filter policy.
2. **Select Time Range** or **Attachment** from the drop-down list.
    - If you choose **Time Range**, the source objects are filtered to be included according to the created time or modified time.
    - If you choose **Attachment**, the attachments within the source objects are filtered to be included according to the size of attachments.
3. Click **Add a Criterion** and the filter rule configuration field appears.
    - For **Time Range**, configure the following settings:
        - In the **Rule** column, select **Created Time** or **Modified Time** from the drop-down list.
        - In the **Condition** column, select **Before**, **After**, **Within**, or **Older Than**.
        - In the **Value** column, set up Time Zone and the exact time by clicking the calendar ( ) button.
    - For **Attachment**, configure the following settings:
        - In the **Condition** column, select **> =** or **< =**.
        - In the **Value** column, enter your desired value and select **KB**, **MB**, or **GB** from the drop-down list.

4. Click the delete ( ) button to delete the specified criterion. You can change the logical relationship between the criterions.

   By default, the logic is set to **And**. If desired, change the logic to **Or** by selecting it from the drop-down list.

   - **And** – The content which meets all the criteria will be filtered to be included.
   - **Or** –The content which meets any one of the criteria will be filtered to be included.

5. Repeat step 1 to step 3 to add more filter criteria.
6. Click **Save** to save your configurations, or click **Cancel** to close the window without saving any configuration.

Performing a Database Analysis

By analyzing the database, you can gather the following kinds of information: Database Basic, Design Statistics, ACL, Content Statistics, Complexity, and Replica Comparison. You can select whether to set the filter to include the information of the documents matching the filter rule.

To analyze the databases, complete the following steps:

1. In the homepage of Lotus Notes Migration, select the databases on the right pane.
2. Choose one of the following methods to access the **Source Data Analysis** window.
   - Click **Analyzer** on the ribbon, and then click **Database Analysis** to select **Source Data Analysis**.
   - Click the source data analysis ( ) button.
   - Right-click a database and click **Source Data Analysis**.
3. Optionally, click the **set up a filter** link to filter the source data for the analysis. For more information, refer to Setting Up Filters.
4. Click **Start Analysis** to start analyzing the source data.
5. The **Analysis Result** section appears with the general database information displayed.
6. Select a specific database from the drop-down list to view detailed information of the database. You can view **Database Basic**, **Design Statistics**, **ACL**, **Content Statistics**, **Complexity**, and **Replica Comparison** in the corresponding tab.
7. Click **Close** to close the **Source Data Analysis** window and go back to the homepage of Lotus Notes Migration.

Setting Up Filters

Use the following filters to include the information of the documents that match the filter rules:

- **Enable size filter** – Select the checkbox and enter the minimum and the maximum document size from the drop-down list.
- **Enable time filter** – Select the checkbox and select the range of the created time and the modified time.
- **Enable form filter** – Select the checkbox. Enter the form name in the text box and click **Add** to add it into the table. To remove a form from the table, click the delete ( ) button that appears at the end of the form name.

  ***Note**: If multiple forms are added into the table, the form filter takes effect when any of the forms is met.

Click **Apply** to apply the filter to source data analysis, or click **Cancel** to close the **Set Up Filter** window without applying any configuration.

Viewing Analysis Report

After analyzing the database, you can check the report for the analyzed database.

In the homepage of Lotus Notes Migration, select one or more databases on the right pane. Then, choose one of the following methods to access the **Analysis Reports** window:

- Click **Analyzer** on the ribbon, and then click **Database Analysis** to select **Analysis Reports**.
- Click the analysis reports () button.
- Right-click a database and click **Analysis Reports**.

In the **Analysis Reports** window, complete the following steps:

1. Select your desired databases on the right pane.
2. In the **Report** drop-down list, select one of the following reports.
   - **Database Summary Report**
   - **Database ACLs Report**
   - **Database Data Element Report**
   - **Database Design Element Report**

   The detailed report information is displayed.
3. Optionally, click **Complexity Illustration** to view the complexity of the database content.
4. Choose one of the following options:

- Click **Export to Excel** to export the report to an Excel file, which resides in *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\AnalysisDataReport*.
- Click **Export to PDF** to export the report to a PDF file, which resides in *…\AvePoint\DocAve6\Agent\data\Migrator\LotusNotesSettings\AnalysisDataReport*.

5. Click **Close** to close the **Analysis Reports** window.

Quickr Migration

On the DocAve Migrator Tool main interface, click **Quickr Migration** to start. In the **Quickr Migration** interface, you can configure content type mapping, user mapping, and scan the source data to determine the potential risks for migration jobs.

Selecting Source

To configure content type mapping, user mapping, and scan analysis, you must select the source first. In the **Quickr Source** section, complete the following steps:

1. Click **Browse…** to select your desired INI file.
2. Select the Quickr version from the **Version** drop-down list.
3. Select **User ID file** from the drop-down list.
4. Enter the password of the selected User ID in the **Password** text box.
5. Click **Load** to load the available Quickr places.
6. Select your desired source node in the left pane.

Performing a Scan Analysis

Before performing a migration job, you can scan the source data to determine the potential risks that may occur in the migration job by completing the following steps:

1. In the homepage of Quickr Migration, click **Scan Analysis** on the right pane.
2. Optionally, select a previously configured filter policy from the drop-down list to filter your desired source objects for the scan, or click **New Filter Policy** to create a new one. Click **Filter Policy Settings** to manage all of the filter policies. For more information, refer to Managing Filter Policies.
3. Configure the options in **Scan Analysis Settings** to define the scan criteria. For each piece of information, you can classify its severity as **Information**, **Warning**, or **Critical**.
    - **Place/Room Risk Information** – Scan the source places and rooms to check whether there are risks for migration.
        - **Place/Room name contains illegal characters** – Check whether there are places or rooms whose names contain illegal characters. Click **Show Details** and the

default illegal characters are displayed. You can add new illegal characters or delete the existing illegal characters.

    - **Form name contains illegal characters** – Check whether there are forms whose names contain illegal characters. Click **Show Details** and the default illegal characters are displayed. You can add new illegal characters or delete the existing illegal characters.

- **Page Risk Information** – Scan the source pages to check whether there are risks for migration.
    - **Unsupported page elements for Quickr Migration** – Check whether there are page elements that are unsupported to be migrated to SharePoint.
- **Folder/File Risk Information** – Scan the source folders and files to check whether there are risks for migration.
    - **Blocked file types in SharePoint** – Check whether there are files types that will be blocked when being migrated to SharePoint. Click **Show Details** and the default blocked file types are displayed. You can add new file types and delete the existing file types.
    - **Length of the folder name exceeds** – Check whether there are folders with folder name lengths exceeding the specified value. By default, the value is **60**. You can define your desired value from 1 to 128.
    - **Length of the file name exceeds** – Check whether there are files with file name lengths exceeding the specified value. By default, the value is **80**. You can define your desired value from 1 to 128.
    - **Length of the SharePoint URL exceeds** – Enter SharePoint library/folder URL in the provided text box and check whether the URLs exceeds the specified value. By default, the value is **255**. You can define your desired value from 1 to 260.
    - **File size exceeds** – Check whether there are files with a size exceeding the specified size. By default, the size is **50 MB**. You can enter your desired value in the text box.
    - **Folder/file name contains illegal characters** – Check whether there are folders or files with names containing illegal characters. Click **Show Details** and the default illegal characters are displayed. You can add new illegal characters and delete the existing illegal characters.
    - **Folder/file name with illegal extension name** – Check whether there are folders or files with names containing illegal extension names. Click **Show Details** and the default illegal extension names are displayed.
    - **Folder/file name contains two consecutive periods (..)** – Check whether there are folders or files with names containing two consecutive periods.

4. Click **Next** to go to the **Scan and Results** step.
5. Click **Browse…** to select a location to store the scan report, and then click **Scan** to start the scan job. You can view the real-time progress.

6. After the scan is completed, the **Scan Analysis Summary** is listed. Go to the specified location to find the scan analysis report and view detailed information.

Managing Filter Policies

To manage filter policies, click **Filter Policy Settings** in the **Scan Analysis Settings** interface. You can create, edit, and delete a filter policy.

- **Create** – Click **Create** on the ribbon to create a new filter policy. For details, refer to Configuring a Filter Policy.
- **Edit** – Select a filter policy and click **Edit** on the ribbon to change the configurations for the selected filter policy. For details, refer to Configuring a Filter Policy.
- **Delete** – Select one or more filter policies and click **Delete** on the ribbon. A confirmation window appears, confirming that you want to proceed with the deletion. Click **OK** to delete the selected filter policies, or click **Cancel** to return to the **Filter Policy** interface without deleting the selected filter policies.

Configuring a Filter Policy

In the **Scan Analysis Settings** interface, select an optional filter policy to filter your desired source objects for the scan. To create a new filter policy, click **New Filter Policy** from the drop-down list and complete the following steps:

1. Enter a **Filter Policy Name** for this filter policy.
2. Click **Add a Criterion** to add a filter criterion based on **Time Range**. The filter rule configuration field appears.
3. In the **Rule** column, select **Created Time** or **Modified Time** from the drop-down list.
4. In the **Condition** column, select **Before**, **After**, **Within**, or **Older Than**.
5. In the **Value** column, set up Time Zone and the exact time by clicking the calendar ( ) button.
6. Click the delete ( ) button to delete the specified criterion. You can change the logical relationship between the criterions.

   By default, the logic is set to **And**. If desired, change the logic to **Or** by selecting it from the drop-down list.

   - **And** – The content which meets all the criteria will be filtered to be included.
   - **Or** –The content which meets any one of the criteria will be filtered to be included.
7. Repeat step 1 to step 5 to add more filter criteria.
8. Click **Save** to save your configurations, or click **Cancel** to close the window without saving any configuration.

Configuring User Mappings

Configure a user mapping to replace the existing source usernames with the existing or default destination usernames. In the homepage of Quickr Migration, click **Create a New User Mapping** on the right pane.

Configuring LDAP Settings

To create a new user mapping, you must configure the LDAP Settings first. To configure LDAP Settings, complete the following steps:

1. Click the **LDAP Settings** link in the **User Mapping** interface. The **LDAP Settings** interface appears.
2. In the **LDAP Settings** interface, the previously configured LDAP paths are displayed in the **Domain** section. If desired, edit or delete the previously configured LDAP.
3. To create a new LDAP, complete the following steps in the **Browse a Domain section**:
    a. **Path** – Enter the IP address or host name where the domain controller is installed.
    b. **Username** – Enter the username in the text box.
    c. **Password** – Enter the password in the text box.
4. Click **Save** to save the current LDAP, or click **Reset** to reset your configurations.

    The saved LDAP path is added into the **Domain** section. You can edit the LDAP setting by selecting the LDAP path and clicking **Edit**. Edit the information in the **Browse a Domain** section. To delete an LDAP setting, select the LDAP path, and then click the delete ( ) button.
5. Click **Close** to close the **LDAP Settings** interface and go back to the **User Mapping** interface.

Creating a User Mapping

To create a new user mapping, complete the following steps:

1. In the **User Mapping** interface, select a domain from the drop-down list and the domain users are loaded in the **Domain Users** pane.
2. Double-click a user. The default user mapping is displayed in the right pane.
3. If you want to modify the default user mapping, double-click the value of **Quickr User**, **SharePoint User**, or **Display Name** to modify.
4. To add a new user mapping, click **Add Row** and enter the required information. To delete a user mapping, select the column, and then click **Delete Row**.
5. Select the checkbox under the **Included** column to include the user in the user mapping.
6. Click **Save** to save your configurations. By default, DocAve saves the configuration file to *…\AvePoint\DocAve6\Agent\data\Migrator\QuickrSettings\UserMapping*.

Creating a Content Type Mapping

Create a content type mapping to map the Quickr form to the specified SharePoint content type. On the Quickr Migration homepage, click **Create a New Content Type Mapping** on the right pane, and then complete the following steps in the **Content Type Mapping Configuration** interface:

1. Select your desired Quickr place or room from the **Place/Room** drop-down list.
2. Select your desired Quickr form in the left pane.
3. Double-click the form and the corresponding Quickr fields are displayed in the right pane.
4. In the **SharePoint Content Type Name** text box, enter the name of the form's corresponding content type in SharePoint.
5. In the **Column Mapping** section, you can modify the default column mapping. Double-click the value of **Quickr Field**, **Quickr Field Type**, or **SharePoint Column** to modify it, and then select a column type from the **SharePoint Column Type** drop-down list.
6. To create a new column, click **Add Row** and enter the required information. To delete an existing column, select the column, and then click **Delete Row**.
7. Click **Export to XML File** to generate and export the content type mapping file. By default, DocAve saves the configuration file to *…\AvePoint\DocAve6\Agent\data\Migrator\QuickrSettings\ContentTypeMapping*.

Editing an Existing Mapping

To edit an previously create user mapping or content type mapping, click **Edit an Existing Mapping** on the right pane in the home page of Quickr Migration.

Select your desired user mapping XML file or content type mapping XML file in the **Edit an Existing Mapping File** window. Then, you are brought to the **User Mapping** or **Content Type Mapping Configuration** interface. For details about configuring a user mapping or content type mapping, refer to Creating a User Mapping or Creating a Content Type Mapping.

eRoom Migration

On the **Migrator Tool** main interface, click **eRoom Migration** to start. For **eRoom Migration**, you can use the migration tool to implement the following functions:

- Scan the source eRoom contents. The contents in the selected nodes will be recorded in the scan report and the contents that match the configured rules will be commented for your reference.
- Configure the security mappings. The configured security mapping settings can be saved to XML files and imported into DocAve Manager for use in running eRoom Migration jobs.

Loading eRoom Structure

To load the eRoom structure, complete the following steps:

1. In the **eRoom Migration** interface, specify a local user in the **eRoom Local System Account** text box and enter the corresponding password in the **Password** text box. Ensure the user you specified can access the eRoom file server. It is recommended to specify the user that you specified when configuring the file server settings during the eRoom installation, or specify the user that is in the local **Administrators** group.
2. Click **Load eRoom Structure** to load the eRoom structure. If you want to display the eRoom templates and scan the contents in the template, select the **Show eRoom templates** checkbox.
3. Expand the data tree and select the desired nodes.

For the selected nodes, refer to the following sections for details of how to configure the security mappings and perform the scan on the source eRoom objects.

Configuring Security Mapping

Before you configure the security mappings, including the domain mapping, group mapping, and user mapping, complete the following steps to configure the LDAP settings first.

1. In the **eRoom Migration** interface, click **Security Mappings** to access the **Security Mappings** interface.
2. Click **LDAP Settings**. The **LDAP Settings** window appears.
3. In the **LDAP Settings** window, enter the following information:
    - **LDAP Path** – Enter the IP address or host name where the domain controller is installed.
    - **Username** – Enter the username that can access the specific domain controller.
    - **Password** – Enter the corresponding password.
4. Click **Add** to add the LDAP settings, or click **Reset** to empty all of the entered information.
5. After the LDAP settings are successfully saved, it appears in the **Domains** field. Click **Close** to return to the **Security Mappings** interface.
6. In the **Security Mappings** interface, you can click **Domain Mapping** to configure the domain mapping settings, click **User Mapping** to configure the user mapping settings, and click **Group Mapping** to configure the group mapping settings. It is recommended to configure the domain mapping settings first before you configure the user mapping settings since the users having the same logon name will be automatically mapped by domain mapping.

Configuring Domain Mapping Settings

In the left pane of the **Domain Mapping** tab, the source domains associated with the selected nodes are displayed in the **Source Domain Name** list. The destination domains are displayed in the **Destination Domain Name** list according to your configurations in the LDAP settings.

To configure the domain mapping settings, complete the following steps:

1. In the left pane, select a source domain from the **Source Domain Name** list and select a destination domain that you want to map the source domain to from the **Destination Domain Name** list.
2. Click **Add** to add the selected source domain and destination domain to the right pane. To remove a domain mapping from the right pane, select the corresponding row and click the delete ( ) button.
3. Click **Export to XML File** to export the domain mappings to a XML file. The user mappings and group mappings configured under the **User Mapping** and **Group Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running eRoom Migration jobs.

   ***Note:** To use the exported mapping file to DocAve Manager, you have to store the exported mapping file in the *...\AvePoint\Agent\data\Migrator\eRoomMigrator* directory.

Configuring User Mapping Settings

To map source users to destination users, configure the user mapping settings in the **User Mapping** tab by completing the following steps:

1. Select one or more eRoom domains from the first drop-down list, click **OK**, and then click **Load**. The **Load Source User** pop-up window appears.
2. In the **Load Source User** interface, choose whether or not to use filter rules to filter and load the desired users. If you select the **Use filter rules** checkbox, complete the following steps to configure the filters:
   a. Click **Add a Criterion** to add a filter rule.
   b. Select **Login Name**, **Display Name**, **First Name**, or **Last Name** from the drop-down list in the **Rule** column.
   c. Select **Starts With** or **Contains** from the drop-down list in the **Condition** column.
   d. Enter the **Value** for this rule.
   e. After configuring one rule, click **Add a Criterion** to add another rule, or click the delete ( ) button following each rule to delete it.
      - If 2 or more rules are configured, select **And** or **Or** from the drop-down list in the **And/Or** column to change the logic relationship between the rules.
   f. Click **Load** to load the source users according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.
3. Select the previously configured LDAP Settings from the second drop-down list under the **User Mapping** tab, and then click **Load**. The **Load Destination User** interface appears.
   a. Click **Add a Criterion** to add a filter rule.

b. Select **Login Name**, **Display Name**, **First Name**, or **Last Name** from the drop-down list in the **Rule** column.

c. Select **Starts With** or **Contains** from the drop-down list in the **Condition** column.

d. Enter the **Value** for this rule.

e. After configuring one rule, click **Add a Criterion** to add another rule, or click the delete ( ) button following each rule to delete it.

- If 2 or more rules are configured, select **And** or **Or** from the drop-down list in the **And/Or** column to change the logic relationship between the rules.

f. Click **Load** to load the destination users according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.

4. You can also click **Add Destination User** to add a new user. It will be created in SharePoint after running the eRoom Migration job. Complete the following steps in the **Add Users** interface:

   a. Click **Add** to add a new user.

   b. Enter the desired username in the text box.

   c. After adding one username, click **Add** to add another username, or click the delete ( ) button to delete this username.

   d. Click **Save** to save your changes or click **Cancel** to return to the **User Mapping** interface.

5. Select a user from the **Source Username** column.
6. Select a user from the **Destination Username** column.
7. Click **Add** to add the user mapping.
8. If desired, select the **Show default matched users** checkbox to automatically match the source user and the destination user whose name are the same. The automatically matched mappings will be displayed in the right pane.
9. Click **Export to XML File** to export the user mappings to a XML file. The domain mappings and group mappings configured under the **Domain Mapping** and **Group Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running eRoom Migration jobs.

   ***Note:** To use the exported mapping file to DocAve Manager, you have to store the exported mapping file in the *...\AvePoint\Agent\data\Migrator\eRoomMigrator* directory.

Configuring Group Mapping

Under the **Group Mapping** tab of the **eRoom Migration** interface, complete the following steps to configure a group mapping:

1. Select one or more eRoom domains from the drop-down list in the left pane, click **OK**, and then click **Load**. The eRoom groups in the selected source domains appear in the **Source Group Name** column.

2. Enter the SharePoint group name in the **Destination Group Name** column at the same row with each of the source eRoom group you want to map to the destination SharePoint nodes.
3. Click **Export to XML File** to export the group mappings to a XML file. The domain mappings and user mappings configured under the **Domain Mapping** and **User Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running eRoom Migration jobs.

   ***Note:** To use the exported mapping file to DocAve Manager, you have to store the exported mapping file in the *...\AvePoint\Agent\data\Migrator\eRoomMigrator* directory.

Performing a Scan Analysis

Scan Analysis is used to scan the source data to determine the potential risks in the eRoom Migration job. To configure the scan analysis settings to set the rules and perform the scan, complete the following steps:

1. Click **Scan Analysis** in the right pane to enter the interface for **Scan Analysis Settings**.
2. Specify a filter policy to filter the desired objects for the scan from the drop-down list or **New Filter Policy** to create a new one. If you do not want to use a filter policy, skip this step. You can also click **Filter Policy Settings** to manage all of the filter policies. For more information on managing filter polies, refer to Managing Filter Policies.
3. Configure the scan analysis settings to set the rules.

   ***Note**: The source contents matching the rules will be marked with a comment in the scan report. For each scan option, select a classification from the **Classification** drop-down list. In the scan report, the contents matching the scan options will be marked with the classification you specified in a **Classification** column, which helps group the scan results.

   - **Block file types in SharePoint** – Scan the files whose file type is blocked in SharePoint. Click **Show Details** to view the blocked types. You can delete or add file types in the list according to your requirements.
   - **Character length** – Scan the contents that exceed the character length limitation. Configure **character** length limitations for SharePoint URL, filename, and folder name. In SharePoint, the maximum length of SharePoint URL is 260 characters, and the maximum length of file name and folder name is 128 characters.
     - **Length of the file name exceeds** – The default value is 60, and the scale you can set is from 1 to 128.
     - **Length of the folder name exceeds** – The default value is 80, and the scale you can set is from 1 to 128. If the character length of the file name (consisting of the file name, the period (.), and extension name) exceeds the limitation you set, the extra characters at end of the file name are pruned.
     - **Length of the SharePoint URL exceeds** – The default value is 255, and the scale you can set is from 1 to 260.The length of the SharePoint URL is calculated from the first character after the "/" in the managed path.

To check whether the length of the SharePoint URL exceeds the limitation, you must specify the length of your destination SharePoint URL by one of the following methods:

  - **Target SharePoint URL** – Enter the URL of the destination SharePoint site.
  - **Target SharePoint URL length** – Enter the length of the destination SharePoint site URL. The length of the SharePoint site URL is calculated from the first character after the "/" in the managed path.

- **File size exceeds** – Scan the files whose size exceeds the specified value. Enter the value in the blank text box. The unit is MB.
- **Item title length exceeds 255 characters** – Scan the items whose title length exceeds 255 characters.
- **Illegal characters in folder/file name in SharePoint** – Scan the files and folders whose name contains the illegal characters. Click **Show Details** to view the illegal characters. You can delete or add illegal characters in the list according to your requirements.
- **Folder/file name with illegal postfixes** – Scan the files and folders whose name ends with illegal postfix. For example, if there is a folder named **abc_bylos**, and **_bylos** is the illegal postfix, this folder will be marked with a comment in the scan report. Click **Show Details** to view the illegal postfixes.
- **Folder/file name contains two consecutive periods (..)** – Scan the files and folders whose name contains consecutive periods.
- **Unsupported contents for migration**– Scan the contents of dashboard and issues tracking (enterprise) database with the **create an enterprise overview** option selected. Both the dashboard and issues tracking (enterprise) database with the **create an enterprise overview** option selected are not supported to be migrated.
- **Checked out files** – Scan the files that are checked out.

4. Click **Next** to enter the **Scan and Results** page.
5. Click **Browse** to specify a storage location for the scan analysis report.
6. Click **Scan** to start scanning.
7. After the scan is finished, click **View Detailed Report** to view the detailed scan analysis report.

Viewing Scan Analysis Report

Open the generated scan analysis report to check the scan results. There are three sheets in the generated tool report: **Summary**, **Migration Risk Analysis**, and **Users and Groups**.

- **Summary** – Includes the number of the scanned eRoom objects sorted according to the object type, the total size of the scanned eRoom objects, and the estimated migration time to migrate all of the scanned eRoom objects to SharePoint using eRoom Migration.
- **Users and Groups** – Includes the names of all of the eRoom users and groups.

- **Migration Risk Analysis** – Includes the URL, name, path, type and size of each scanned eRoom object, the facility and room where the scanned eRoom object resides, the creator, creator's e-mail, created time, last modifier, last modified time of the scanned eRoom object, whether the scanned eRoom object is checked out, the estimated level of the risks when migrating the scanned eRoom object, and the suggestions to reduce the risks.

Managing Filter Policies

In the **Scan Analysis Settings** interface, click **Filter Policy Settings** to go to **Filter Policy** interface. All of the previously configured filter policies are displayed in this interface. You can create, edit, or delete filter policies in this interface.

- **Create** – Click **Create** on the ribbon to create a new filter policy. For details, refer to Configuring a Filter Policy.
- **Edit** – Select a filter policy and click **Edit** on the ribbon to change the configurations for the selected filter policy.
- **Delete** – Select one or more filter policies and click **Delete** on the ribbon. A confirmation window appears, confirming that you want to proceed with the deletion. Click **OK** to delete the selected filter policies, or click **Cancel** to return to the **Filter Policy** interface without deleting the selected filter policies.

Configuring a Filter Policy

To create a new filter policy, click **New Filter Policy** from the drop-down list in the **Scan Analysis Settings** interface or click **Create** in the **Filter Policy** interface. The **Create** interface appears. Configure the following settings:

1. Enter a name for your filter policy in the **Filter Policy Name** text box.
2. Select **File** from the drop-down list in the lower-left corner, and then click **Add a Criterion**.
    - **Order** – Double-click the value in the **Order** column, and then you can adjust the order of the filter rules of the same level.
    - **Rule** – Select a rule from the drop-down list in the **Rule** column.
    - **Condition** – Select a condition from the drop-down list in the **Condition** column.
    - **Value** – Specify a value in the **Value** column.
3. After configuring one rule, click **Add a Criterion** to add another rule, or click the delete ( ) button following each rule to delete the rule.
    - If 2 or more rules are configured, determine the logical relationship between the rules by double-clicking the value in the **And/Or** column following each rule, and choosing **And** or **Or** from the drop-down list.

4. Click **Save** to save your changes and return to the **Filter Policy** interface, or click **Cancel** to return to the **Filter Policy** interface without saving any changes. The newly created filter policy is displayed in the **Filter Policy** interface.

Livelink Migration

On the DocAve Migrator Tool homepage, click **Livelink Migration** to start. For Livelink Migration, you can use the tool to scan the source data to view the data information, configure the domain/user/group mapping and save the mapping settings to XML file, and perform the simple database queries.

Performing a Scan Analysis

To use the Livelink Migration tool, complete the following steps:

1. Navigate to **DocAve Migrator Tool** > **Livelink Migration**. The **Connection Management** interface appears. All of the previously created Livelink connections are displayed in this interface.
2. Click **New Livelink Connection** to create a new Livelink connection. The **New Livelink Connection** pop-up window appears.
3. Enter the name for the connection in the **Livelink connection name** text box.
4. In the **Use HTTP tunneling** field, select **Yes** to use the Http Tunneling connection mode, or select **No** to use the default connection mode.
    - **Http Tunneling**
        - **Proxy option** – Select to use **Web server** or **Proxy server** to access to Livelink.
            - **Web server** – If you select **Web server**, specify the hostname or IP address of the Web server in the **Web server** text box.
            - **Proxy server** – If you select **Proxy server**, specify the hostname or IP address of the Proxy server in the **Proxy server** text box.
        - **Port** – Specify the port the server is using.
        - **Livelink CGI URL** – Enter the Livelink CGI URL.
        - **Livelink username** – Enter a Livelink username for accessing Livelink.
        - **Livelink password** – Enter the corresponding password.
        - **Livelink domain** – Enter the Livelink domain name. If the specified Livelink user is in the Livelink system domain, leave this option blank.
        - **HTTP username** – Enter the HTTP username and the password to set up access to the Web server**.**
        - **HTTP password** – Enter the corresponding password.
    - **Default**
        - **Livelink server** – Enter the hostname or IP address of the Livelink server.

- **Port** – Specify the port the server is using.
- **Livelink username** – Enter the Livelink username for accessing Livelink.
- **Livelink password** – Enter the corresponding password.
- **Livelink domain** – Enter the Livelink domain name. If the specified Livelink user is in the Livelink system domain, leave this value blank.

5. In the **Livelink Database Connection** field, select **Yes** to configure Livelink database connection or keep the default **No** if you do not want to configure the Livelink database connection.

   To view the detailed Livelink database information, you can navigate to **Livelink Administration** > **Database Administration** > **Maintain Current Database**, and then enter the appropriate information.

   ***Note**: Livelink stores all data in the Livelink Database, but DocAve Livelink Migrator can load most of the data by using the API (Application Programming Interface). If you do not configure the Livelink database connection, the following content cannot be migrated.

   - Best Bets Value/ Best Bets Expiry
   - Poll Results

   To configure the Livelink Database Connection, enter the obtained information in the corresponding checkboxes:

   - **Oracle Server** – Select this option if your Livelink database is in the Oracle Server.
     - **Database name** – Enter the obtained **Service Name**.
     - **Schema owner** – Enter the obtained **User Name**.
     - **Username** – Enter the username to access the obtained **Service Name**.
     - **Password** – Enter the corresponding password.

     ***Note:** To save the Livelink connection successfully, make sure the Oracle client is installed on the server where DocAve Migrator Tool resides.

   - **Microsoft SQL Server** – Select this option if your Livelink database is in the Microsoft SQL Server.
     - **Database server name** – Enter the obtained **SQL Server Name**.
     - **Database name** – Enter the obtained **SQL Server Database**.
     - **Schema owner** – Enter the obtained **User Name**.
     - **Username** – Enter the username used to connect to the obtained **SQL Server Name**.
     - **Password** – Enter the corresponding password.

6. Select the **Create another** checkbox if you want to create another connection after this connection has been saved.

7. Click **Save** to save the configurations and return to the **Connection Management** interface. The newly created Livelink connection is displayed in the **Connection Management** interface.
8. Hover over the Livelink connection record and click the **Edit** link to edit the connection or click the delete ( ) button to delete the connection.
9. Click **Next** to proceed. The **Source Data Selection** interface appears.
10. Select a connection from the **Specify a Livelink connection** drop-down list. The source data is loaded on the data tree.
11. Select the Livelink objects you are about to scan by selecting the corresponding checkboxes, and then click **Next**.
12. In the **Scan Analysis Settings** interface, configure the following settings:

    - **Filter Policy Settings** – Filters the desired Livelink objects for the scan. Select an existing filter policy from the drop-down list or click **New Filter Policy** to create a new one. Click **Filter Policy Settings** to manage all of the filter policies. For more information, refer to Managing Filter Policies.
    - **Blocked file types in SharePoint** – Scans the Livelink file types that are blocked by SharePoint. If you select this checkbox, the tool will scan the file types that are blocked by SharePoint and then report these files in the **Scan Analysis Report**.
        - Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list. This is used to identify the severity of this issue.
        - Click **Show Details** and the default blocked file types are displayed. You can add new file types and delete the existing file types. Use a semicolon between two file types.
    - **Target SharePoint URL** – Enter the URL of the destination SharePoint node. It is used to calculate the URL length of the Livelink objects after they are migrated to SharePoint.
    - **Character Length** – Specify the character length of the file name, folder name, and SharePoint URL in the corresponding text boxes, and then select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list to identify the severity of this issue.
    - **File size exceeds _ (MB)** – Specify a maximum file size, and then select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list.
    - **Item title length exceeds 255 characters** – Scans whether or not the item title exceeds 255 characters. Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list.
    - **Illegal characters in folder/file name in SharePoint** – Scans whether or not there are illegal characters in folder/file names. Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list. Click **Show Details** and the default illegal characters are displayed. You can add new illegal characters or delete the existing illegal characters. Use a space between two illegal characters.

- **Folder name ended with illegal suffixes** – Scans whether or not there are folder name ended with illegal suffixes. Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list. Click **Show Details** to view detailed illegal suffixes.
- **The file or folder name contains two consecutive periods (..), starts with a period (.), or ends with a period (.) –** Scans whether or not the file or folder name contains two consecutive periods, starts with a period, or ends with a period. Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list.
- **Unsupported contents for Livelink Migration –** Scans whether or not there are unsupported Livelink objects. Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list.
- **Checked-Out files** – Scans whether or not there are checked-out files. Select **Critical**, **Warning**, or **Information** from the **Classification** drop-down list.

13. Select one of the following options to perform:
    - **Reset** – Resets the customized settings in the **Scan Analysis Settings** interface to the default values.
    - **Back** – Returns to the previous interface.
    - **Next** – Saves the configurations and proceed to the next step.
    - **New Scan** – Creates a new scan without saving any configurations.
14. If you click **Next**, the **Scan and Results** interface appears. Click **Browse** to specify a storage location for the scan analysis report.
15. If you want to use the database connection to scan, select the **Use database connection to scan** checkbox.
16. Click **Scan** to start the scan.
17. After the scan is finished, click **View Detailed Report** to view the directory of the scan analysis report. If desired, go to the corresponding directory to view the detailed report.

Scan Analysis Report

Open the generated scan analysis report to check the scan results. There are three sheets in the generated tool report: **Summary**, **Migration Risk Analysis**, and **Users and Groups**.

- **Summary** – Includes the number of the scanned Livelink objects sorted according to the object type, the total size of the scanned Livelink objects, and the estimated migration time to migrate all the scanned Livelink objects to SharePoint using Livelink migrator.
- **Migration Risk Analysis** – Includes the URLs of the scanned Livelink objects, the names of the scanned Livelink objects, the workspace where the scanned Livelink objects reside, the information about whether or not the scanned Livelink objects reside in personal workspace, the last modified times of the scanned Livelink objects, the types of the scanned Livelink objects, the estimated level of the risks when migrating the scanned Livelink objects, and the suggestions to reduce the risks.

- **Users and Groups** – Includes the names of all Livelink users and groups.

Managing Filter Policies

In the **Scan Analysis Settings** interface, click **Filter Policy Settings** to go to **Filter Policy** interface. All of the previously configured filter policies are displayed in this interface. You can create, edit, or delete filter policies in this interface.

- **Create** – Creates a new filter policy.
- **Edit** – Edits an existing filter policy.
- **Delete** – Deletes one or more filter policies.

Click **Create** to create a new filter policy. The **Create** interface appears. Configure the following settings:

1. Enter a name for your filter policy in the **Filter Policy Name** text box.
2. Select **Item**, **List**, or **Version** from the drop-down list in the lower-left corner, and then click **Add a Criterion**.
   - **Order** – Double-click the value in the **Order** column, and then you can adjust the order of the filter rules of the same level.
   - **Rule** – Select a rule from the drop-down list in the **Rule** column.
   - **Condition** – Select a condition from the drop-down list in the **Condition** column.
   - **Value** – Specify a value in the **Value** column.
   - **And/Or** – If there are two or more filter rules, click the value in the **And/Or** column, and then you can choose **And** or **Or** from the drop-down list to adjust the logical relationship of the filter rules of the same level.
   - **Delete** – Click the delete ( ) button to delete the specific filter rule.

   For more information about filter policy examples, refer to Filter Policy Examples.
3. Click **Save** to save your changes and return to the **Filter Policy** interface or click **Cancel** to return to the **Filter Policy** interface without saving any changes. The newly created filter policy is displayed in the **Filter Policy** interface.

Filter Policy Examples

Refer to the following tables on the examples of the filter policy.

Item Level

Refer to the following table for the filter rules and conditions on the **Item** filter level.

Rule	Condition	Value	Example
Name	Contains	Livelink	The Livelink items whose name contains Livelink will be filtered and included in the filter result.

Rule	Condition	Value	Example
	Does Not Contain	Livelink	The Livelink items whose name does not contain Livelink will be filtered and included in the filter result.
	Equals	Livelink	The Livelink items whose name equals Livelink will be filtered and included in the filter result.
	Does Not Equal	Livelink	The Livelink items whose name does not equal Livelink will be filtered and included in the filter result.
Size	>=	80 KB	The Livelink items whose size are larger than or equal to 80 KB will be filtered and included in the filter result.
	<=	80 KB	The Livelink items whose size are smaller than or equal to 80 KB will be filtered and included in the filter result.
Owner	Contains	user	The Livelink items owned by the user whose name contains user will be filtered and included in the filter result.
	Does Not Contain	user	The Livelink items owned by the user whose name does not contain user will be filtered and included in the filter result.
	Equals	user	The Livelink items owned by the user whose name equals user will be filtered and included in the filter result.
	Does Not Equal	user	The Livelink items owned by the user whose name does not equal user will be filtered and included in the filter result.
Created By	Contains	user	The Livelink items owned by the user whose name contains user will be filtered and included in the filter result.
	Does Not Contain	user	The Livelink items owned by the user whose name does not contain user will be filtered and included in the filter result.
	Equals	user	The Livelink items owned by the user whose name equals user will be filtered and included in the filter result.
	Does Not Equal	user	The Livelink items owned by the user whose name does not equal user will be filtered and included in the filter result.
Metadata: Text	Contains	Livelink	The specified Text attribute of the Livelink items whose values contain Livelink will be filtered and included in the filter result.
	Does Not Contain	Livelink	The specified Text attribute of the Livelink items whose values do not contain Livelink will be filtered and included in the filter result.

Rule	Condition	Value	Example
	Equals	Livelink	The specified Text attribute of the Livelink items whose values equal Livelink will be filtered and included in the filter result.
	Does Not Equal	Livelink	The specified Text attribute of the Livelink items whose values do not equal Livelink will be filtered and included in the filter result.
Metadata: Number	>=	6	The specified Number attribute of the Livelink items whose values are larger than or equal to 6 will be filtered and included in the filter result.
	<=	6	The specified Number attribute of the Livelink items whose values are smaller than or equal to 6 will be filtered and included in the filter result.
	=	6	The specified Number attribute of the Livelink items whose values are equal to 6 will be filtered and included in the filter result.
Metadata: Yes/No	Is Exactly	Yes	The specified Yes/No attribute of the Livelink items whose values are Yes will be filtered and included in the filter result.
Metadata: Date and Time	Before	Wednesday, December 4, 2013 (UTC-08:00)	The specified Date and Time attribute of the Livelink items whose values are before Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	After	Wednesday, December 4, 2013 (UTC-08:00)	The specified Date and Time attribute of the Livelink items whose values are after Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	Within	5 Days	The specified Date and Time attribute of the Livelink items whose values are within 5 days will be filtered and included in the filter result.
	Older Than	5 Days	The specified Date and Time attribute of the Livelink items whose values are older than 5 days will be filtered and included in the filter result.
Created Time	Before	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink items whose created time is before Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	After	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink items whose created time is after Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	Within	5 Days	The Livelink items whose created time is within 5 days will be filtered and included in the filter result.
	Older Than	5 Days	The Livelink items whose created time is older than 5 days will be filtered and included in the filter result.

Rule	Condition	Value	Example
Modified Time	Before	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink items whose modified time is before Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	After	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink items whose modified time is after Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	Within	5 Days	The Livelink items whose modified time is within 5 days will be filtered and included in the filter result.
	Older Than	5 Days	The Livelink items whose modified time is older than 5 days will be filtered and included in the filter result.

List Level

Refer to the following table for the filter rules and conditions on the **List** filter level.

***Note:** The Livelink objects in the lists that are filtered and excluded from the filter result will not be scanned and included in the **Scan Analysis Report**.

Rule	Condition	Value	Example
Name	Contains	Livelink	The Livelink lists whose name contains Livelink will be filtered and included in the filter result.
	Does Not Contain	Livelink	The Livelink lists whose name does not contain Livelink will be filtered and included in the filter result.
	Equals	Livelink	The Livelink lists whose name equals Livelink will be filtered and included in the filter result.
	Does Not Equal	Livelink	The Livelink lists whose name does not equal Livelink will be filtered and included in the filter result.
Description	Contains	Livelink	The Livelink lists whose description contains Livelink will be filtered and included in the filter result.
	Does Not Contain	Livelink	The Livelink lists whose description does not contain Livelink will be filtered and included in the filter result.
	Equals	Livelink	The Livelink lists whose description equals Livelink will be filtered and included in the filter result.
	Does Not Equal	Livelink	The Livelink lists whose description does not equal Livelink will be filtered and included in the filter result.
Created By	Contains	user	The Livelink lists created by the user whose name contains user will be filtered and included in the filter result.
	Does Not Contain	user	The Livelink lists created by the user whose name does not contain user will be filtered and included in the filter result.

Rule	Condition	Value	Example
	Equals	user	The Livelink lists created by the user whose name equals user will be filtered and included in the filter result.
	Does Not Equal	user	The Livelink lists created by the user whose name does not equal user will be filtered and included in the filter result.
Owned By	Contains	user	The Livelink lists owned by the user whose name contains user will be filtered and included in the filter result.
	Does Not Contain	user	The Livelink lists owned by the user whose name does not contain user will be filtered and included in the filter result.
	Equals	user	The Livelink lists owned by the user whose name equals user will be filtered and included in the filter result.
	Does Not Equal	user	The Livelink lists owned by the user whose name does not equal user will be filtered and included in the filter result.
Created Time	Before	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink lists whose created time is before Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	After	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink lists whose created time is after Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	Within	5 Days	The Livelink lists whose created time is within 5 days will be filtered and included in the filter result.
	Older Than	5 Days	The Livelink lists whose created time is older than 5 days will be filtered and included in the result.
Modified Time	Before	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink lists whose modified time is before Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	After	Wednesday, December 4, 2013 (UTC-08:00)	The Livelink lists whose modified time is after Wednesday, December 4, 2013 (UTC-08:00) will be filtered and included in the filter result.
	Within	5 Days	The Livelink lists whose modified time is within 5 days will be filtered and included in the filter result.
	Older Than	5 Days	The Livelink lists whose modified time is older than 5 days will be filtered and included in the filter result.

Version Level

Refer to the following table for the filter rules and conditions on the **Version** filter level.

Rule	Condition	Value	Example
Document Version	Only Latest [] Versions	2	The latest two versions of the Livelink documents will be filtered and included in the filter results.

Rule	Condition	Value	Example
Compound Document Release	Only Latest [] Versions	2	The latest two Release versions of the Livelink compound documents will be filtered and included in the filter results.
Compound Document Revision	Only Latest [] Versions	2	The latest two Revision versions of the Livelink compound documents will be filtered and included in the filter results.

Configuring Security Mappings

Security Mappings include **Domain Mapping**, **User Mapping**, and **Group Mapping**. Click **Security Mappings** tab to go to the **Security Mappings** interface.

Configuring LDAP Settings

Before configuring the security mappings, you must configure **LDAP Settings** first by completing the following steps:

1. Click the **LDAP Settings** link. The **Configure LDAP Settings** pop-up window appears.
2. In the **Configure LDAP Settings** interface, configure the following settings:
    - **LDAP Path** – Enter the IP address or hostname where the domain controller is installed.
    - **Username** – Enter the username that can access the specific domain controller.
    - **Password** – Enter the corresponding password.
3. Click **Add** to add the LDAP setting, or click **Reset** to empty all of the entered information.
4. After the LDAP settings are successfully saved, it appears in the **Domains** field. Click **Close** to return to the **Security Mappings** interface.

Configuring Domain Mappings

Under the **Domain Mapping** tab of the **Security Mappings** interface, complete the following steps to configure a domain mapping:

1. Select a previously configured Livelink connection from the drop-down list, and then click **Load** to load the source domains.
    - **Source Domain Name** – Displays all of the loaded source domains.
    - **Destination Domain Name** – Displays all of the previously configured LDAP settings.
2. Select a domain from the Source Domain Name column, and then select a domain from the **Destination Domain Name** column.
3. Click **Add** to add the selected source domain and destination domain to the right pane.
4. Click **Export to XML File** to export the domain mappings to a XML file. The user mappings and group mappings configured under the **User Mapping** and **Group Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running Livelink Migration jobs.

***Note:** To use the exported mapping file to DocAve Manager, you have to store the exported mapping file in the *…\AvePoint\Agent\data\Migrator\LivelinkMigrator* directory.

Configuring User Mappings

Under the **User Mapping** tab of the **Security Mappings** interface, complete the following steps to configure a user mapping:

1. Select one or more Livelink domains from the first drop-down list, click **OK**, and then click **Load**. The **Load Source User** pop-up window appears.
2. In the **Load Source User** interface, choose whether or not to use filter rules to filter and load the desired users. If you select the **Use filter rules** checkbox, complete the following steps to configure the filters:
    a. Click **Add a Criterion** to add a filter rule.
    b. Select **Login Name**, **Display Name**, **First Name**, or **Last Name** from the drop-down list in the **Rule** column.
    c. Select **Starts With**, **Contains**, or **By Regex** from the drop-down list in the **Condition** column. For more information, refer to Filter Rules Examples.
    d. If there are two or more filter rules, select **Add** or **Or** from the drop-down list in the **Add/Or** column to change the logic relationship of rules. You can click the delete ( ) button to delete the specific rule.
    e. Click **Load** to load the source users according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.
3. Select the previously configured LDAP Settings from the second drop-down list under the **User Mapping** tab, and then click **Load**. The **Load Destination User** interface appears.
    a. Click **Add a Criterion** to add a filter rule.
    b. Select **Login Name**, **Display Name**, **First Name**, or **Last Name** from the drop-down list in the **Rule** column.
    c. Select **Starts With**, **Contains**, or **By Regex** from the drop-down list in the **Condition** column. For more information, refer to Filter Rules Examples.
    d. If there are two or more filter rules, select **Add** or **Or** from the drop-down list in the **Add/Or** column to change the logic relationship of rules. You can click the delete ( ) button to delete the specific rule.
    e. Click **Load** to load the destination users according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.
4. You can also click **Add a Destination User** to add a new user.
    a. In the **Add Users** interface, click **Add** to add a new user.

b. Enter the desired username in the text box.

c. You can click the delete ( ) button to delete the specific user.

d. Click **Save** to save your changes or click **Cancel** to return to the **User Mapping** interface.

5. Select a user from the **Source Username** column.
6. Select a user from the **Destination Username** column.
7. Click **Add** to add the user mapping.
8. If desired, select the **Show default matched users** checkbox to automatically match the source user and the destination user whose name are the same. The automatically matched mappings will be displayed in the right pane.
9. Click **Export to XML File** to export the user mappings to a XML file. The domain mappings and the group mappings configured on the **Domain Mapping** tab and the **Group Mapping** tabs are also exported to the other two XML files. You can import these XML file to DocAve Manager and use them while running Livelink Migration jobs.

   ***Note:** To use the exported mapping file to DocAve Manager, you have to store the exported mapping file in the *...\AvePoint\Agent\data\Migrator\LivelinkMigrator* directory.

Configuring Group Mappings

Under the **Group Mapping** tab of the **Security Mappings** interface, complete the following steps to configure a group mapping:

1. Select one or more Livelink domains from the first drop-down list, click **OK**, and then click **Load**. The **Load Source Group** pop-up window appears.
2. In the **Load Source Group** interface, choose whether or not to use filter rules to filter and load the desired groups. If you select the **Use filter rules** checkbox, complete the following steps to configure the filters:

   a. Click **Add a Criterion** to add a filter rule.

   b. Select **Starts With**, **Contains**, or **By Regex** from the drop-down list in the **Condition** column. For more information, refer to Filter Rules Examples.

   c. If there are two or more filter rules, select **Add** or **Or** from the drop-down list in the **Add/Or** column to change the logic relationship of rules. You can click the delete ( ) button to delete the specific rule.

   d. Click **Load** to load the source groups according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.

3. Select the previously configured LDAP Settings from the second drop-down list under the **Group Mapping** tab, and then click **Load**. The **Load Destination Group** interface appears.

   a. Click **Add a Criterion** to add a filter rule.

b. Select **Starts With**, **Contains**, or **By Regex** from the drop-down list in the **Condition** column. For more information, refer to Filter Rules Examples.

c. If there are two or more filter rules, select **Add** or **Or** from the drop-down list in the **Add/Or** column to change the logic relationship of rules. You can click the delete ( ) button to delete the specific rule.

d. Click **Load** to load the destination groups according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.

4. You can also click **Add a Destination Group** to add a new group. It will be created in SharePoint after running the Livelink Migration job.

   a. In the **Add Groups** interface, click **Add** to add a new group.

   b. Enter the desired group name in the text box.

   c. You can click the delete ( ) button to delete the specific group.

   d. Click **Save** to save your changes, or click **Cancel** to return to the **Group Mapping** interface.

5. Select a group from the **Source Group Name** column.
6. Select a user from the **Destination Group Name** column.
7. Click **Add** to add the group mapping.
8. If desired, select the **Show default matched groups** checkbox to automatically match the source group and the destination group whose name are the same. The automatically matched mappings will be displayed in the right pane.
9. Click **Export to XML File** to export the group mappings to a XML file. The domain mappings and the user mappings configured on the **Domain Mapping** tab and the **User Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running Livelink Migration jobs.

   ***Note:** To use the exported mapping file to DocAve Manager, you have to store the exported mapping file in the *...\AvePoint\Agent\data\Migrator\LivelinkMigrator* directory.

Filter Rules Examples

Refer to the following table for the examples of the filter rules in the **Load Source User** or **Load Destination User** interface.

Rule	Condition	Value	Example
Login Name	Starts With	L	All of the source or destination users whose login name starts with L will be filtered and included in the filter result.
	Contains	L	All of the source or destination users whose login name contains L will be filtered and included in the filter result.
	By Regex	l*	All of the source or destination users whose login name begins with T will be filtered and included in the filter result.

Rule	Condition	Value	Example
Display Name	Starts With	L	All of the source or destination users whose display name starts with L will be filtered and included in the filter result.
	Contains	L	All of the source or destination users whose display name contains L will be filtered and included in the filter result.
	By Regex	t*	All of the source or destination users whose display name begins with t will be filtered and included in the filter result.
First Name	Starts With	L	All of the source or destination users whose first name starts with L will be filtered and included in the filter result.
	Contains	L	All of the source or destination users whose first name contains L will be filtered and included in the filter result.
	By Regex	t*	All of the source or destination users whose first name begins with t will be filtered and included in the filter result.
Last Name	Starts With	L	All of the source or destination users whose last name starts with L will be filtered and included in the filter result.
	Contains	L	All of the source or destination users whose last name contains L will be filtered and included in the filter result.
	By Regex	t*	All of the source or destination users whose last name begins with t will be filtered and included in the filter result.

Refer to the following table for the examples of the filter rules in the **Load Source Group** or **Load Destination Group** interface.

Rule	Condition	Value	Example
Group Name	Starts With	L	All of the source or destination groups whose group name starts with L will be filtered and included in the filter result.
	Contains	L	All of the source or destination groups whose group name contains L will be filtered and included in the filter result.
	By Regex	t*	All of the source or destination groups whose group name begins with t will be filtered and included in the filter result.

Configuring Database Inquiry

Use **Database Inquiry** to perform some simple queries on the Livelink database. To access **Database Inquiry**, click **Database Inquiry** tab. The **Database Inquiry** interface appears. Before you start to perform the queries, you must create a database connection by completing the following steps:

1. In the **Database Inquiry** interface, click **Create Database Connection**. The **Create Livelink Database Connection** pop-up window appears.
2. To view the detailed Livelink database information, you can navigate to Livelink Administration > Database Administration > Maintain Current Database, and then enter the appropriate information.

   ***Note**: Livelink stores all data in the Livelink Database, but DocAve Livelink Migrator can load most of the data by using the API (Application Programming Interface). If you do not configure the Livelink database connection, the following content cannot be migrated.

- Best Bets Value/ Best Bets Expiry
- Poll Results

3. To configure the Livelink Database Connection, enter the obtained information in the corresponding checkboxes of the **Create Livelink Database Connection** interface:
    - **Oracle Server** – Select this option if your Livelink database is in the Oracle Server.
        - **Database name** – Enter the obtained **Service Name**.
        - **Schema owner** – Enter the obtained **User Name**.
        - **Username** – Enter the username to access the obtained **Service Name**.
        - **Password** – Enter the corresponding password.

      ***Note:** To save the Livelink connection successfully, make sure the Oracle client is installed on the server where DocAve Migrator Tool resides.

    - **Microsoft SQL Server** – Select this option if your Livelink database is in the Microsoft SQL Server.
        - **Database server name** – Enter the obtained **SQL Server Name**.
        - **Database name** – Enter the obtained **SQL Server Database**.
        - **Schema owner** – Enter the obtained **User Name**.
        - **Username** – Enter the username used to connect to the obtained **SQL Server Name**.
        - **Password** – Enter the corresponding password.
4. Click **Save** to save your configurations, or click **Cancel** to return to the **Database Inquiry** interface without saving any changes.
5. Select the desired node from the tree.
6. Enter a SQL statement in the **Enter Database Query** text box.
7. Click **Query** to execute the entered SQL statement. The query results are shown in the field under the **Query** button.

   ***Note:** Only the **Select** SQL statement is supported here.

EMC Documentum Migration

In the Migrator Tool main interface, click **EMC Documentum Migration** to start. For EMC Documentum Migration, you can use the migration tool to implement the following functions:

- Scan the source EMC Documentum contents. The contents in the selected nodes will be recorded in the scan report and the contents that match the configured rules will be marked with a comment for your reference.

- Configure the security mappings. This tool can export the configured security mapping settings to XML files and you can import these XML files to DocAve for use in running migration jobs.
- Configure the content type mapping. This tool can export the configured content type mapping settings to an XML file and DocAve can use this XML file in migration jobs.

Configuring EMC Documentum Connection

To use EMC Documentum Migration, you must configure the EMC Documentum connection so that the tool can access the specified repository in EMC Documentum.

1. In the **EMC Documentum Migration** interface, click **EMC Documentum Connection Management**. The **EMC Documentum Connection Management** window appears.
    - **Connection Name** – Enter a name in the text box for the EMC Documentum connection.
    - **Login Name** and **Password –** Enter the user's login name and password for accessing the specified repository.
    - **Repository** – Enter the repository name in the text box. DocAve Agent will connect to the repository you specified here.
    - **Domain** – If the repository is running on the domain-required mode, enter the domain name.
2. When you complete the settings, Click **Save** to validate and save the connection settings, or click **Reset** to reset the connection settings. You can create multiple connections.
3. Close the **EMC Documentum Connection Management** window to return to the **EMC Documentum Migration** interface.
4. Select a previously configured EMC Documentum connection from the **Specify an EMC Documentum Connection** drop-down list. The selected connection appears in the left pane for specifying the scope for future operations.

Specifying Source

To configure content type mapping, security mappings, and scan analysis, you must select the source first by completing the following steps:

1. In the left pane of the **EMC Documentum Migration** interface, expand the selected EMC Documentum connection to load all of the available cabinet nodes.
2. Click on the cabinet nodes to expand the data tree and select your desired nodes.

For the selected nodes, refer to the following sections for details on how to configure the Scan Analysis, Security Mappings and Content Type Mapping.

Performing a Scan Analysis

Scan Analysis is used to scan the source data to determine the potential risks in the EMC Documentum migration job. To configure the scan analysis settings to set the rules and perform the scan, complete the following steps:

1. Click **Scan Analysis** in the right pane to enter the interface for Scan Analysis Settings.
2. Specify a filter policy to filter the desired objects for the scan from the drop-down list, or select **New Filter Policy** to create a new one. If you do not want to use a filter policy, skip this step. You can also click **Filter Policy Settings** to manage all of the filter policies. For more information on managing filter polies, refer to Managing Filter Policies.
3. Configure the scan analysis settings to set the rules.

   ***Note**: The source contents matching the rules will be marked with a comment in the scan report. For each scan option, select a classification from the **Classification** drop-down list. In the scan report, the contents matching the scan options will be marked with the classification you specified in a Classification column, which helps group the scan results.

   - **Blocked file types in SharePoint** – Scan the files with a file type that is blocked in SharePoint. Click **Show Details** to view the blocked types. You can delete or add file types in the list according to your requirements.
   - **Character Length** – Scan the contents that exceed the character length limitation. Configure character length limitations for file name, folder name, and SharePoint URL. In SharePoint, the maximum length of SharePoint URL is 260 characters, and the maximum length of file name and folder name is 128 characters.
   - **Length of the file name exceeds** – The default value is 80, and the scale you can set is from 1 to 128.
   - **Length of the folder name exceeds** – The default value is 60, and the scale you can set is from 1 to 128. If the character length of the file name (consisting of the file name, the period (.), and extension name) exceeds the limitation you set, the extra characters at end of the file name are pruned.
   - **Length of the SharePoint URL exceeds** – The default value is 255, and the scale you can set is from 1 to 260.The length of the SharePoint URL is calculated from the first character after the "/" in the managed path.

     To check whether the length of the SharePoint URL exceeds the limitation, you must specify the length of your destination SharePoint URL by one of the following methods:

     - **Target SharePoint URL** – Enter the URL of the destination SharePoint site.
     - **Target SharePoint URL length** – Enter the length of the destination SharePoint site URL. The length of the SharePoint site URL is calculated from the first character after the "/"in the managed path.
   - **File size exceeds** – Scan the files whose size exceeds the specified value. Enter the value in the blank text box. The default value is 50 and the unit is MB.

- **Source column value exceeds 255 characters or is before the year 1900** – Scan the items whose column value exceeds 255 characters or is before the year 1900.
- **Illegal characters in folder/file name in SharePoint** – Scan the files and folders whose name contains the illegal characters. Click **Show Details** to view the illegal characters. You can delete or add illegal characters in the list according to your requirements.
- **Folder/File name with illegal postfixes** – Scan the files and folders whose name ends with illegal postfix. For example, if there is a folder named **abc_bylos**, and **_bylos** is the illegal postfix, this folder will be marked with a comment in the scan report. Click **Show Details** to view the illegal postfixes. You can delete or add illegal postfixes in the list according to your requirements.
- **Folder/File name contains two consecutive periods (..)** – Scan the files and folders whose name contains consecutive periods.
- **Unsupported Content** – Scan the contents that are not supported for migration, including the nested virtual documents, nested snapshots and the files that meet both of the following criteria:
    - File size is 0 KB.
    - File is required to be exported during the migration
- **Checked out Files** – Scan the files that are checked out.
- **Incompatible version numbers** – Scan the file with a version number that is incompatible with the SharePoint version number.
- **Rendition files** – Scan the rendition files of the source files.

4. Click **Next** to enter the **Scan and Results** page.
5. Click **Browse** to specify a storage location for the scan analysis report.
6. Click **Scan** to start scanning.
7. After the scan is finished, click **View Detailed Report** to view the detailed scan analysis report.

Viewing Scan Analysis Report

Open the generated scan analysis report to check the scan results. There are three sheets in the generated tool report: **Summary**, **Migration Risk Analysis**, and **Users and Groups**.

- **Summary** – Includes the number of the scanned EMC Documentum objects sorted according to the object type, the total size of the scanned EMC Documentum objects, and the estimated migration time to migrate all of the scanned EMC Documentum objects to SharePoint using EMC Documentum migration.
- **Users and Groups** – Includes the names of all of the EMC Documentum users and groups.
- **Migration Risk Analysis** – Includes the URL and name of each scanned EMC Documentum object, the repository and cabinet where the scanned EMC Documentum object resides, the creator, created time, last modifier, last modified time of the

scanned EMC Documentum object, whether the scanned EMC Documentum object is checked out, the type, format, and size of the scanned EMC Documentum object, the estimated level of the risks when migrating the scanned EMC Documentum object, and the suggestions to reduce the risks.

Managing Filter Policies

In the **Scan Analysis Settings** interface, click **Filter Policy Settings** to go to **Filter Policy** interface. All of the previously configured filter policies are displayed in this interface. You can create, edit, or delete filter policies in this interface.

- **Create** – Click **Create** on the ribbon to create a new filter policy. For details, refer to Configuring a Filter Policy.
- **Edit** – Select a filter policy and click **Edit** on the ribbon to change the configurations for the selected filter policy.
- **Delete** – Select one or more filter policies and click **Delete** on the ribbon. A confirmation window appears, confirming that you want to proceed with the deletion. Click **OK** to delete the selected filter policies, or click **Cancel** to return to the **Filter Policy** interface without deleting the selected filter policies.

Configuring a Filter Policy

To create a new filter policy, click **New Filter Policy** from the drop-down list in the **Scan Analysis Settings** interface or click **Create** in the **Filter Policy** interface. The **Create** interface appears. Configure the following settings:

1. Enter a name for your filter policy in the **Filter Policy Name** text box.
2. Select **Folder**, or **File** from the drop-down list in the lower-left corner, and then click **Add a Criterion**.
    - **Order** – Double-click the value in the **Order** column, and then you can adjust the order of the filter rules of the same level.
    - **Rule** – Select a rule from the drop-down list in the **Rule** column.
    - **Condition** – Select a condition from the drop-down list in the **Condition** column.
    - **Value** – Specify a value in the **Value** column.
3. After configuring one rule, click **Add a Criterion** to add another rule, or click the delete (✕) button following each rule to delete the rule.
    - If 2 or more rules are configured, determine the logical relationship between the rules at the same level by double-clicking the value in the **And/Or** column following each rule, and choosing **And** or **Or** from the drop-down list.
4. Click **Save** to save your changes and return to the **Filter Policy** interface, or click **Cancel** to return to the **Filter Policy** interface without saving any changes. The newly created filter policy is displayed in the **Filter Policy** interface.

Configuring Security Mapping

Security Mappings include **Domain Mapping**, **User Mapping**, and **Group Mapping**. Click **Security Mappings** in the **EMC Documentum** interface to go to the **Security Mappings** interface.

Configuring LDAP Settings

Before you configure the security mapping, including the domain mapping, group mapping, and user mapping, complete the following steps to configure the LDAP settings first.

1. In the **EMC Documentum Migration** interface, click **LDAP Settings**. The **LDAP Settings** window appears.
2. In the **LDAP Settings** window, configure the following settings:
    - **LDAP Path** – Enter the IP address or host name where the domain controller is installed.
    - **Username** – Enter the username that can access the specific domain controller.
    - **Password** – Enter the corresponding password.
3. Click **Add** to add the LDAP setting, or click **Reset** to empty all of the entered information.
4. After the LDAP settings are successfully saved, it appears in the **Domains** field. Click **Close** to return to the **Security Mappings** interface.

Configuring Domain Mappings

Under the **Domain Mapping** tab of the **Security Mappings** interface, complete the following steps to configure a domain mapping:

1. Select a domain from the **Source Domain Name** column, and then select a domain from the **Destination Domain Name** column.
2. Click **Add** to add the selected source domain and destination domain to the right pane.
3. Click **Export to XML File** to export the domain mappings to a XML file. The user mappings and group mappings configured under the **User Mapping** and **Group Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running EMC Documentum Migration jobs.

Configuring User Mapping Settings

To map source users to destination users, configure the user mapping settings in the **User Mapping** tab by completing the following steps:

1. Select one or more EMC Documentum domains from the first drop-down list, click **OK**, and then click **Load**. The **Load Source User** pop-up window appears.
2. In the **Load Source User** interface, choose whether or not to use filter rules to filter and load the desired users. If you select the **Use filter rules** checkbox, complete the following steps to configure the filters:

a. Click **Add a Criterion** to add a filter rule.

b. Select **Login Name** or **Display Name** from the drop-down list in the **Rule** column.

c. Select **Starts With** or **Contains** from the drop-down list in the **Condition** column.

d. Enter the **Value** for this rule.

e. After configuring one rule, click **Add a Criterion** to add another rule, or click the delete () button following each rule to delete it.

- If 2 or more rules are configured, select **And** or **Or** from the drop-down list in the **And/Or** column to change the logic relationship between the rules.

f. Click **Load** to load the source users according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.

3. Select the previously configured LDAP Settings from the second drop-down list under the **User Mapping** tab, and then click **Load**. The **Load Destination User** interface appears.

a. Click **Add a Criterion** to add a filter rule.

b. Select **Login Name** or **Display Name** from the drop-down list in the **Rule** column.

c. Select **Starts With** or **Contains** from the drop-down list in the **Condition** column.

d. Enter the **Value** for this rule.

e. After configuring one rule, click **Add a Criterion** to add another rule, or click the delete () button following each rule to delete it.

- If 2 or more rules are configured, select **And** or **Or** from the drop-down list in the **And/Or** column to change the logic relationship between the rules.

f. Click **Load** to load the destination users according to the filter rules, or click **Cancel** to exit the current page without saving any configurations.

4. You can also click **Add a Destination User** to add a new user. It will be created in SharePoint after running the EMC Documentum Migration job.

a. In the **Add Users** interface, click **Add** to add a new user.

b. Enter the desired username in the text box.

c. You can click the delete () button to delete the specific user.

d. Click **Save** to save your changes, or click **Cancel** to return to the **User Mapping** interface.

5. Select a user from the **Source Username** column.

6. Select a user from the **Destination Username** column.

7. Click **Add** to add the user mapping.

8. If desired, select the **Show default matched users** checkbox to automatically match the source user and the destination user whose name are the same. The automatically matched mappings will be displayed in the right pane.
9. Click **Export to XML File** to export the user mappings to a XML file. The domain mappings and group mappings configured under the **Domain Mapping** and **Group Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running EMC Documentum Migration jobs.

Configuring Group Mapping

Under the Group Mapping tab of the EMC Documentum interface, complete the following steps to configure a group mapping:

1. Select one or more EMC Documentum domains from the drop-down list in the left pane, click **OK**, and then click **Load**. The EMC Documentum groups in the selected source domains appear in the **Source Group Name** column.
2. Enter the SharePoint group name or Active Directory domain group name in the **Destination Group Name** column at the same row with each of the source EMC Documentum group you want to map to the destination SharePoint nodes.
3. Click **Export to XML File** to export the group mappings to a XML file. The domain mappings and user mappings configured under the **Domain Mapping** and **User Mapping** tabs are also exported to the other two XML files. You can import these XML files to DocAve Manager and use them while running EMC Documentum Migration jobs.

Configuring Content Type Mapping

Configure content type mapping settings to map EMC Documentum types to SharePoint content types. Complete the following steps to configure content type mapping settings:

In the homepage of **EMC Documentum Migration**, click **Content Type Mapping** in the right pane. Then, complete the following steps in the **Content Type Mapping** interface:

1. In the **Folder Types** and **Document Type**s fields, select the desired folder types and/or document types that you want to perform the configurations.
2. Click **Next** to go to the **Configure Content Type Mapping** interface.
3. In the left **EMC Documentum Types** field, expand the tree to select a type for configuring content type mappings.
4. The right field displays the information for this type.
    - **Content Type Mapping** – Configure the content type name mapping.
        - **EMC Documentum Folder/Document Type** – Displays the selected type's name.
        - **SharePoint Content Type** – Enter the destination content type name.
    - **Column Mapping** – Configure the column mapping settings.
        - **EMC Documentum Attribute Name** – Displays the source attribute name.

- **SharePoint Column Name** – Enter the destination column name.
- **SharePoint Column Type** – Select a column type from the drop-down list.
- **Migrate Column** – Select whether to use this column mapping settings in this content type mapping. Select the checkbox to use it and migrate the source attribute, and uncheck the checkbox to not use it and not migrate the source attribute.
- **Add To Default View** – Specify whether to add this SharePoint column to the default view by selecting/unchecking the checkbox.

5. Click **Export to XML File** to save the content type mapping settings and generate and export the content type mapping file. By default, this tool generates the **DocumentumMigrationTypeMapping.xml** file in the *…AvePoint\DocAve6\Agent\data\Migrator\DocumentumMigrator\TypeMappings* directory. To make sure DocAve can use this generated mapping settings in migration jobs when the **Use the content type mapping generated by Migrator Tool** option is selected in the DocAve 6 > **EMC Documentum Migration** > **Profile Settings** > **Mapping Options** > **Content Type Mapping** interface, do not move this file to other locations. You can also further edit the content type mapping settings in the exported XML file by selecting the **Manually configure the content type mapping** option in the DocAve 6 > **EMC Documentum Migration** > **Profile Settings** > **Mapping Options** > **Content Type Mapping** interface and uploading the desired XML file.

Notices and Copyright Information

Notice
The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright
Copyright ©2012-2015 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA